

Installationshandbuch

Revision B

McAfee® Email Gateway 7.x – Appliances

Inhaltsverzeichnis

Einleitung

Dieses Handbuch enthält die Informationen, die Sie zum Installieren Ihres McAfee-Produkts benötigen.

Inhalt

Informationen zu diesem Handbuch

In diesem Abschnitt werden die Zielgruppe des Handbuchs, die verwendeten typografischen Konventionen und Symbole sowie die Gliederung des Handbuchs beschrieben.

Zielgruppe

Die Dokumentation von McAfee wird inhaltlich sorgfältig auf die Zielgruppe abgestimmt.

Die Informationen in diesem Handbuch richten sich in erster Linie an:

- **Administratoren** – Personen, die das Sicherheitsprogramm eines Unternehmens implementieren und umsetzen.

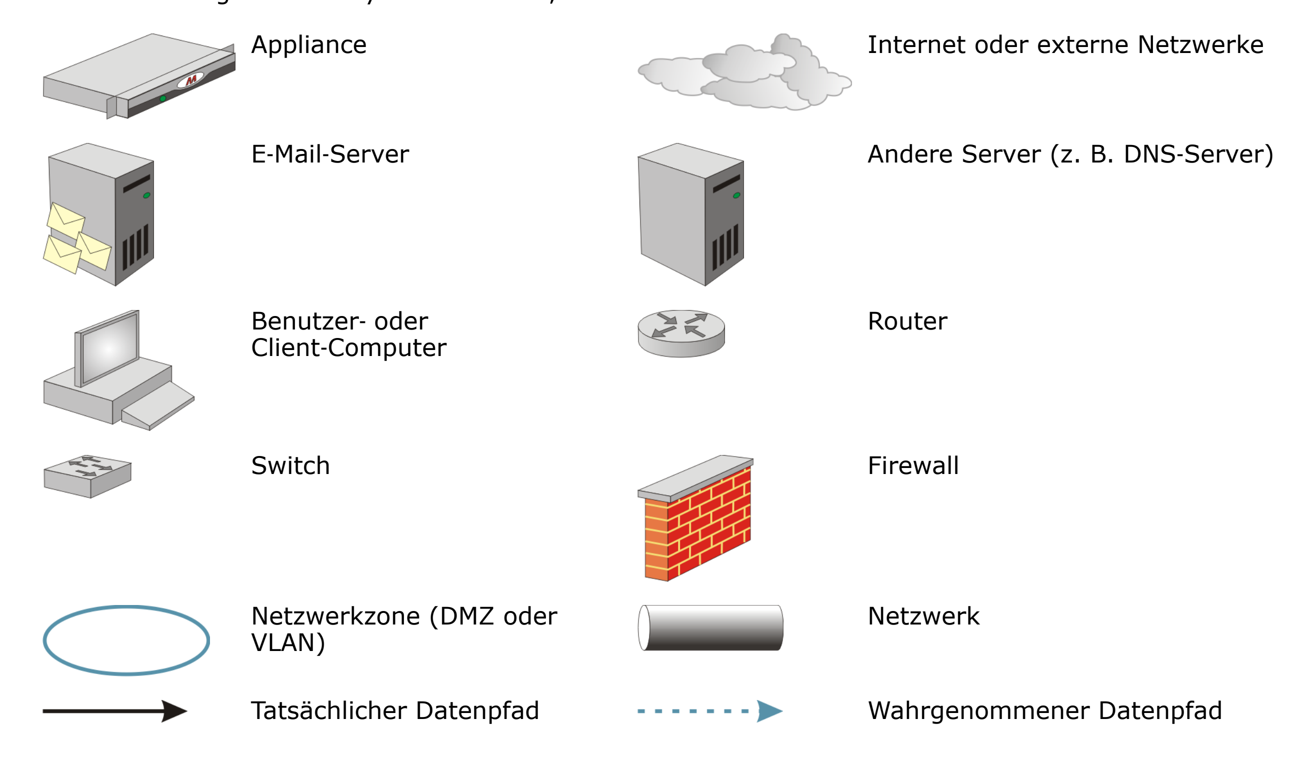
Konventionen

In diesem Handbuch werden folgende typografische Konventionen und Symbole verwendet.

Buchtitel, *Begriff*, *Hervorhebung*	Titel eines Buchs, Kapitels oder Themas; ein neuer Begriff; eine Hervorhebung.
Fett	Text, der stark hervorgehoben wird.
`Benutzereingabe, Code, Meldung`	Befehle oder andere Texte, die vom Benutzer eingegeben werden; ein Code-Beispiel; eine angezeigte Meldung.
Benutzeroberflächentext	Wörter aus der Benutzeroberfläche des Produkts, z. B. Optionen, Menüs, Schaltflächen und Dialogfelder.
Hypertext-Blau	Ein Link auf ein Thema oder eine externe Website.
	Hinweis: Zusätzliche Informationen, beispielsweise eine alternative Methode für den Zugriff auf eine Option.
	Tipp: Vorschläge und Empfehlungen.
	Wichtig/Vorsicht: Wichtige Ratschläge zum Schutz Ihres Computersystems, der Software-Installation, des Netzwerks, Ihres Unternehmens oder Ihrer Daten.
	Warnung: Wichtige Ratschläge, um körperliche Verletzungen bei der Nutzung eines Hardware-Produkts zu vermeiden.

Graphische Konventionen

Lernen Sie die grafischen Symbole kennen, die in diesem Dokument verwendet werden.



Definition der Begriffe in diesem Handbuch

Lernen Sie einige der Schlüsselbegriffe kennen, die in diesem Dokument verwendet werden.

Begriff	Beschreibung
Demilitarisierte Zone (DMZ)	Ein Computer-Host oder kleineres Netzwerk, das als Puffer zwischen ein privates Netzwerk und das äußere öffentliche Netzwerk eingefügt wurde, um den direkten Zugriff durch außenstehende Benutzer auf Ressourcen im privaten Netzwerk zu verhindern.
DAT-Dateien	Erkennungsdefinitionsdateien (DAT), auch als Signaturdateien bezeichnet, enthalten die Definitionen, die Viren, Trojaner, Spyware, Adware und andere potenziell unerwünschte Programme (PUPe) identifizieren, erkennen und entfernen.
Betriebsmodus	Es gibt drei Betriebsmodi für das Produkt: "Expliziter Proxy", "Transparente Bridge" und "Transparenter Router".
Richtlinie	Eine Sammlung der Sicherheitskriterien (z. B. Konfigurationseinstellungen, Benchmarks und Spezifikationen für den Netzwerkzugriff), die die erforderliche Compliance-Stufe für Benutzer, Geräte und Systeme definieren, die von einer McAfee-Sicherheitsanwendung bewertet oder erzwungen werden kann.
Reputationsdienst-Prüfung	Teil der Absenderauthentifizierung. Wenn ein Absender die Reputationsdienst-Prüfung nicht besteht, ist die Appliance so eingestellt, dass die Verbindung beendet und die Nachricht nicht zugelassen wird. Die IP-Adresse des Absenders wird zu einer Liste blockierter Verbindungen hinzugefügt und in Zukunft automatisch auf Kernel-Ebene blockiert.

Verwendung dieses Handbuchs

Dieser Abschnitt enthält eine kurze Zusammenfassung der in diesem Dokument enthaltenen Informationen.

In diesem Handbuch wird Folgendes behandelt:

- Planung und Ausführung Ihrer Installation.
- Umgang mit der Benutzeroberfläche.
- Testen der ordnungsgemäßen Funktion des Produkts.
- Anwendung der aktuellsten Erkennungsdefinitionsdateien.
- Vertrautmachen mit einigen Scan-Richtlinien, Erstellen von Berichten und Abrufen der Statusinformationen.
- Beheben einiger grundlegender Probleme.

Weitere Informationen über die Scan-Funktionen des Produkts finden Sie in der Online-Hilfe des Produkts und in der aktuellen Version des *McAfee Email Gateway-Administratorhandbuches*.

Quellen für Produktinformationen

McAfee stellt Ihnen die Informationen zur Verfügung, die Sie in den einzelnen Phasen der Produktimplementierung benötigen – von der Installation bis hin zur täglichen Nutzung und Fehlerbehebung. Nach der Produktveröffentlichung erhalten Sie Informationen zu diesem Produkt online in der KnowledgeBase von McAfee.

Vorgehensweise

1. Wechseln Sie zum McAfee Technical Support ServicePortal unter http://mysupport.mcafee.com.
2. Greifen Sie unter **Self Service** (Online-Support) auf die erforderlichen Informationen zu:

Zugriff auf	Vorgehensweise
Benutzerdokumentation	1 Klicken Sie auf **Product Documentation** (Produktdokumentation). 2 Wählen Sie ein Produkt und dann eine Version aus. 3 Wählen Sie ein Produktdokument aus.
KnowledgeBase	• Klicken Sie auf **Search the KnowledgeBase** (KnowledgeBase durchsuchen), um Antworten auf Ihre produktbezogenen Fragen zu erhalten. • Klicken Sie auf **Browse the KnowledgeBase** (KnowledgeBase durchblättern), um Artikel nach Produkt und Version aufzulisten.

1 Vorbereitung der Installation

Um den sicheren Betrieb Ihres McAfee Email Gateway Appliance zu gewährleisten, sollten Sie folgende Punkte vor Beginn der Installation bedenken.

- Machen Sie sich mit den Betriebsmodi und den Funktionen vertraut. Es ist wichtig, dass Sie eine gültige Konfiguration auswählen.
- Entscheiden Sie, wie Sie die Appliance in Ihr Netzwerk integrieren möchten, und stellen Sie fest, welche Informationen Sie benötigen, bevor Sie beginnen. Sie benötigen beispielsweise den Namen und die IP-Adresse des Geräts.
- Packen Sie das Produkt so nah wie möglich am vorgesehenen Aufstellungsort aus.
- Nehmen Sie das Produkt aus der Schutzverpackung, und stellen Sie es auf eine ebene Fläche.
- Beachten Sie alle Sicherheitswarnungen.



Lesen Sie alle mitgelieferten Sicherheitsinformationen, und machen Sie sich mit ihnen vertraut.

Inhalt

Lieferumfang

Stellen Sie mithilfe dieser Informationen sicher, dass die Lieferung des Produkts vollständig ist.

Überprüfen Sie anhand der mit dem Produkt ausgelieferten Packliste, ob alle Komponenten enthalten sind.

Folgendes sollte vorhanden sein:

- Eine Appliance
- Netzkabel
- Netzwerkkabel
- Installations- und Wiederherstellungs-CD für McAfee Email Gateway
- CD mit dem Linux-Quellcode
- Dokumentations-CD

Wenn ein Element fehlt oder beschädigt ist, setzen Sie sich mit dem Händler in Verbindung.

Planen der Installation

Nutzen Sie diese Informationen, um die Installation des Geräts zu planen.

Bevor Sie das McAfee Email Gateway auspacken, sollten Sie unbedingt die Installation und Ausbringung planen.

Beachten Sie Folgendes:

- Umgebungsanforderungen

  Informationen zu den Umgebungsanforderungen, einschließlich Temperatur, Belüftung und Platzbedarf.

- Stromanforderungen und Überlegungen

  Stromanforderungen und elektrische Faktoren, die vor der Installation bedacht werden müssen.

- Hardware-Spezifikationen und -Anforderungen
- Konfigurationsszenarien
- Vorbereiten der Installation

Nicht bestimmungsgemäße Nutzung

Erfahren Sie, wie Sie vermeiden, das Produkt nicht bestimmungsgemäß zu nutzen.

McAfee Email Gateway ist:

- **Keine Firewall** – Es muss in Ihrer Organisation hinter einer ordnungsgemäß konfigurierten Firewall verwendet werden.
- **Kein Server zum Speichern zusätzlicher Software und Dateien** – Installieren Sie keine Software auf dem Gerät, und fügen Sie keine zusätzlichen Dateien hinzu, es sei denn, Sie werden in der Produktdokumentation oder von Ihrem Support-Mitarbeiter dazu aufgefordert.



Das Gerät kann nicht alle Arten von Datenverkehr verarbeiten. Wenn Sie den Modus „Expliziter Proxy" verwenden, sollten nur Protokolle an das Gerät gesendet werden, die gescannt werden müssen.

Betriebsbedingungen

In diesem Abschnitt lernen Sie die Umgebungsbedingungen kennen, die für das McAfee Email Gateway erforderlich sind.

Betriebstemperatur	+10 °C bis + 30 °C oder +10 °C bis + 35 °C (modellabhängig), wobei die Änderungsgeschwindigkeit maximal 10 °C pro Stunde beträgt
Lagerungstemperatur	-40 °C bis +70 °C
Relative Feuchtigkeit bei Lagerung	90 %, nicht kondensierend bei 35 °C
Vibration, unverpackt	5 Hz bis 500 Hz, 2,20 g RMS regellos
Erschütterung, im Betrieb	Halbsinus, 2 g Höchstwert, 11 m/Sek

Erschütterung, unverpackt trapezoid	25 g, Geschwindigkeitsänderung 3,45 m/Sek. (≧18,1 kg bis > 36,3 kg)
Kühlbedarf des Systems in Watt	486,38 W oder 747,15 W (modellabhängig)

Platzieren der Appliance

In diesem Abschnitt erfahren Sie, wo das McAfee Email Gateway platziert werden sollte, bevor es eingerichtet und verwendet wird.

Berücksichtigen Sie bei der Wahl des endgültigen Aufstellungsorts und der Installation folgende Gesichtspunkte: die Betriebsbedingungen werden eingehalten, der physische Zugang zur Appliance ist kontrollierbar und die Anschlüsse und Verbindungen auf der Vorder- und Rückwand sind zugänglich.

Im Lieferumfang der Appliance ist ein Set zur Montage in einem Rack enthalten, mit dem Sie die Appliance in einem 19-Zoll-Rack installieren können.

Überlegungen zu Netzwerkmodi

In diesem Abschnitt lernen Sie die Betriebsmodi (Netzwerkmodi) kennen, in denen das Gerät betrieben werden kann.

Bevor Sie das McAfee Email Gateway installieren und konfigurieren, müssen Sie sich überlegen, welchen Netzwerkmodus Sie verwenden möchten. Vom ausgewählten Modus hängt es ab, wie Sie Ihre Appliance physisch an Ihr Netzwerk anschließen.

Sie können einen der folgenden Netzwerkmodi auswählen:

- **Modus "Transparente Bridge"** – Das Gerät fungiert als Ethernet-Bridge.
- **Modus "Transparenter Router"** – Das Gerät fungiert als Router.
- **Modus "Expliziter Proxy"** – Das Gerät fungiert als Proxyserver und Mail-Relay.

Wenn Sie nach der Lektüre dieses und der folgenden Abschnitte weiterhin unsicher sind, welchen Modus Sie verwenden sollen, sprechen Sie mit einem Netzwerkexperten.

Architektonische Aspekte hinsichtlich der Netzwerkmodi

Hinsichtlich der Netzwerkmodi müssen Sie vor allem folgende Aspekte bedenken:

- Ob Kommunikationsgeräte die Existenz des Geräts kennen. Das heißt, ob das Gerät in einem der transparenten Modi arbeitet.
- Wie das Gerät physisch mit Ihrem Netzwerk verbunden wird.
- Die erforderliche Konfiguration zur Integration des Geräts in Ihr Netzwerk.
- An welchem Ort im Netzwerk die Konfiguration erfolgt.

Überlegungen vor dem Ändern des Netzwerkmodus

In den Modi "Expliziter Proxy" und "Transparenter Router" können Sie das Gerät so einrichten, dass es sich innerhalb mehrerer Netzwerke befindet. Dies wird durch das Einrichten mehrerer IP-Adressen für die LAN1- und LAN2-Anschlüsse ermöglicht.

Wenn Sie aus dem Modus "Expliziter Proxy" oder "Transparenter Router" in den Modus "Transparente Bridge" wechseln, wird nur die aktivierte IP-Adresse für jeden Anschluss übernommen.



Nachdem ein Netzwerkmodus festgelegt wurde, empfiehlt es sich, diesen nicht mehr zu ändern, es sei denn, der Standort des Geräts ändert sich oder das Netzwerk wird neu strukturiert.

Modus "Transparente Bridge"

In diesem Abschnitt lernen Sie den Modus "Transparente Bridge" des McAfee Email Gateways besser kennen.

Im Modus "Transparente Bridge" bemerken die kommunizierenden Server das Gerät nicht. Der Betrieb des Geräts ist für die Server transparent.

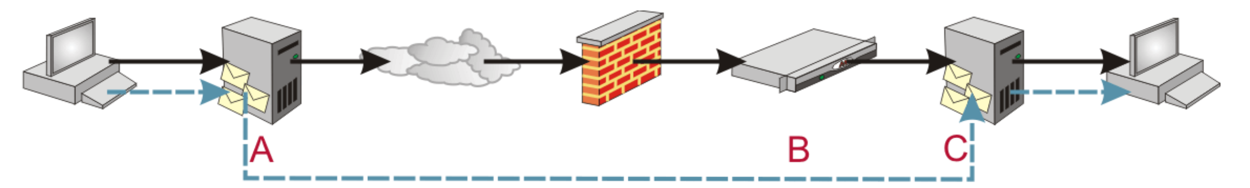


Abbildung 1-1 Modus "Transparente Bridge" – sichtbarer Datenpfad

In der Abbildung sendet der externe E-Mail-Server (**A**) E-Mail-Nachrichten an den internen E-Mail-Server (**C**). Der externe Mail-Server kann nicht erkennen, dass die von ihm gesendete E-Mail-Nachricht vom Gerät abgefangen und gescannt wird (**B**).

Der externe E-Mail-Server scheint direkt mit dem internen E-Mail-Server zu kommunizieren (der Pfad wird als gestrichelte Linie dargestellt). Tatsächlich wird der Datenverkehr möglicherweise durch mehrere Netzwerkgeräte geleitet und vom Gerät abgefangen und gescannt, bevor er den internen Mail-Server erreicht.

Arbeitsweise des Geräts im Modus "Transparente Bridge"

Im Modus "Transparente Bridge" wird das Gerät über den LAN1- und den LAN2-Anschluss mit dem Netzwerk verbunden. Das Gerät scannt den empfangenen Datenverkehr und fungiert als Bridge, die zwei Netzwerksegmente verbindet, behandelt diese aber wie ein einziges logisches Netzwerk.

Konfiguration im Modus "Transparente Bridge"

Der Modus "Transparente Bridge" erfordert weniger Konfigurationsaufwand als die Modi "Transparenter Router" oder "Expliziter Proxy". Sie müssen nicht alle Clients, das Standard-Gateway, MX-Einträge, Firewall-NAT und E-Mail-Server neu konfigurieren, damit der Datenverkehr an das Gerät gesendet wird. Da das Gerät in diesem Modus nicht als Router fungiert, ist es auch nicht erforderlich, eine Routing-Tabelle zu aktualisieren.

Platzieren des Geräts bei Betrieb im Modus "Transparente Bridge"

Aus Sicherheitsgründen sollten Sie das Gerät innerhalb Ihres Unternehmens und hinter einer Firewall betreiben.

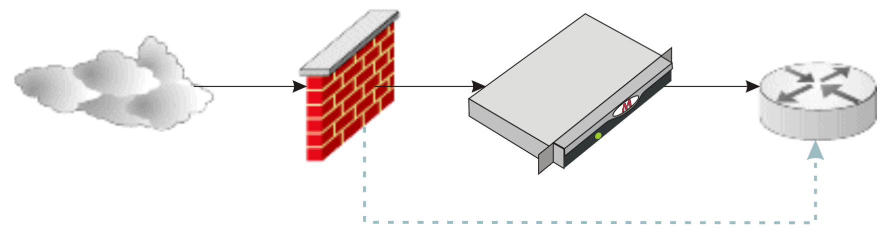


Abbildung 1-2 Platzierung im Modus "Transparente Bridge"



Platzieren Sie das Gerät im Modus "Transparente Bridge" zwischen der Firewall und Ihrem Router, wie in der Abbildung dargestellt.

In diesem Modus verbinden Sie zwei Netzwerksegmente physisch mit dem Gerät. Das Gerät behandelt diese als eine einzige logische Einheit. Da sich die Geräte – Firewall, Gerät und Router – im selben logischen Netzwerk befinden, müssen sie kompatible IP-Adressen im selben Subnetz haben.

Geräte auf der einen Seite der Bridge (z. B. ein Router), die mit den Geräten auf der anderen Seite der Bridge (z. B. einer Firewall) kommunizieren, bemerken die Bridge nicht. Sie erkennen nicht, dass der Datenverkehr abgefangen und gescannt wird. Deshalb wird dieser Betriebsmodus des Geräts als "Transparente Bridge" bezeichnet.

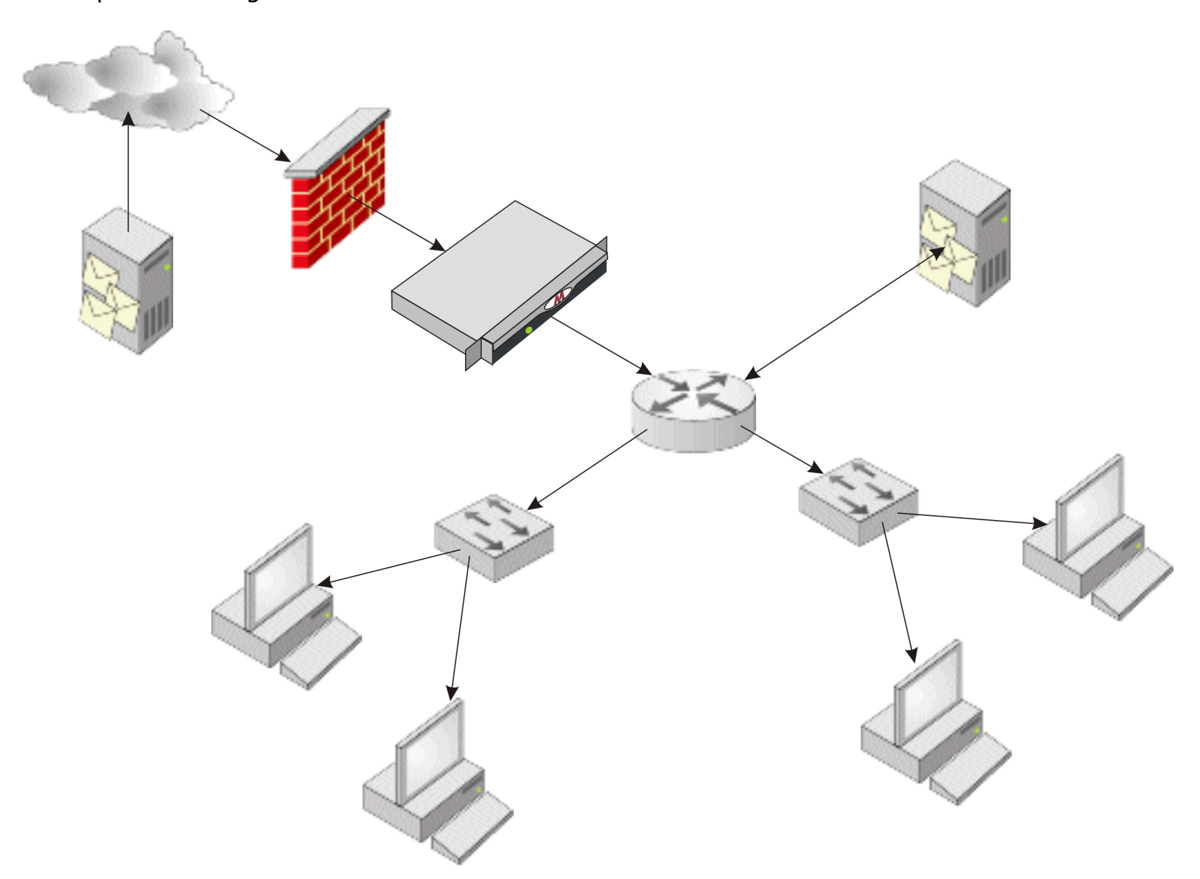


Abbildung 1-3 Netzwerkstruktur – Modus "Transparente Bridge"

Modus "Transparenter Router"

In diesem Abschnitt lernen Sie den Modus "Transparenter Router" des McAfee Email Gateways besser kennen.

Im Modus "Transparenter Router" scannt das Gerät den E-Mail-Verkehr zwischen zwei Netzwerken. Das Gerät hat eine IP-Adresse für ausgehenden gescannten Verkehr und muss eine IP-Adresse für eingehenden Verkehr haben.

Die kommunizierenden Netzwerkserver erkennen nicht, dass das Gerät zwischengeschaltet ist. Der Betrieb des Geräts ist für die Geräte transparent.

Arbeitsweise des Geräts im Modus "Transparente Router"

Im Modus "Transparenter Router" wird das Gerät mit den Netzwerken über den LAN1- und den LAN2-Anschluss verbunden. Das Gerät scannt den Datenverkehr, der über ein Netzwerk eingeht, und leitet ihn an das nächste Netzwerkgerät in einem anderen Netzwerk weiter. Das Gerät fungiert als Router (wobei es Datenverkehr zwischen den verschiedenen Netzwerken auf der Basis der Informationen in den Routing-Tabellen weiterleitet).

Konfiguration im Modus "Transparenter Router"

Im Modus "Transparenter Router" müssen Sie Ihre Netzwerkgeräte nicht explizit neu konfigurieren, damit der Datenverkehr an das Gerät gesendet wird. Sie müssen lediglich die Routing-Tabelle für das Gerät konfigurieren und einige der Routing-Informationen für die Netzwerkgeräte auf einer Seite des Geräts ändern (der Geräte also, die an die LAN1- und LAN2-Anschlüsse des Geräts angeschlossen sind). Es könnte zum Beispiel erforderlich sein, das Gerät als Standard-Gateway zu konfigurieren.

Im Modus "Transparenter Router" muss das Gerät zwei Netzwerke miteinander verbinden. Das Gerät muss innerhalb Ihres Unternehmens hinter einer Firewall platziert werden.



Im Modus "Transparenter Router" werden weder Multicast-IP-Datenverkehr noch andere Protokolle wie NETBEUI und IPX (Nicht-IP-Protokolle) unterstützt.

Firewall-Regeln

Im Modus "Transparenter Router" wird die Firewall mit der physischen IP-Adresse für die LAN1/LAN2-Verbindung mit dem Management-Blade-Server verbunden.

Platzieren des Geräts

Verwenden Sie das Gerät im Modus "Transparenter Router", um einen im Netzwerk vorhandenen Router zu ersetzen.



Wenn Sie den Modus "Transparenter Router" verwenden und keinen vorhandenen Router ersetzen, müssen Sie einen Teil Ihres Netzwerks neu konfigurieren, damit der Datenverkehr korrekt durch das Gerät fließt.

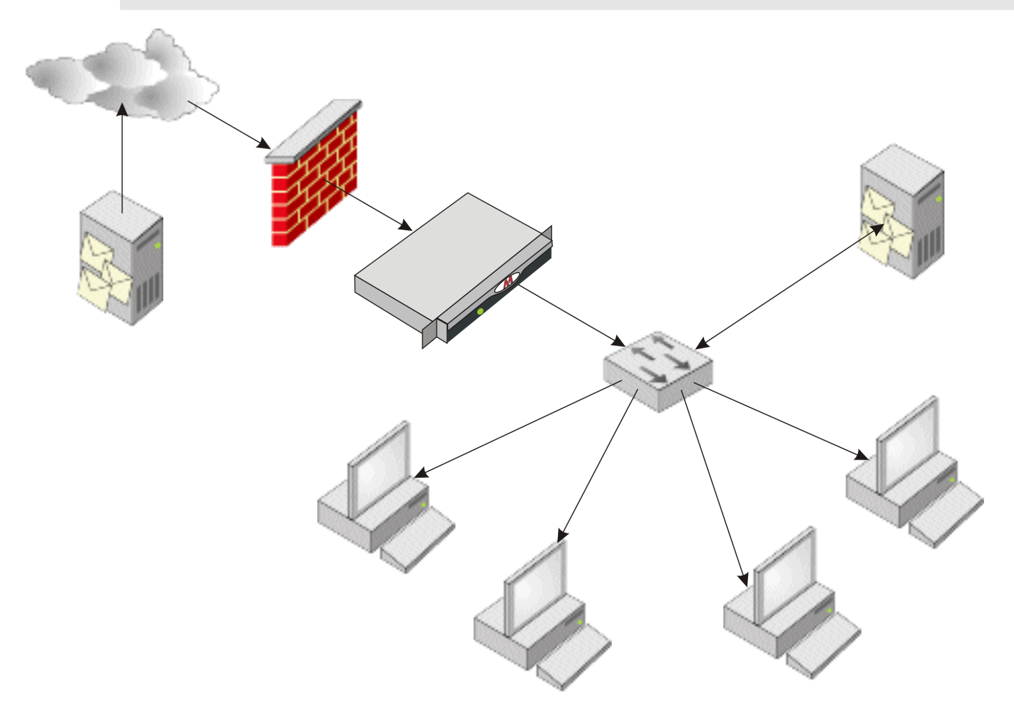


Abbildung 1-4 Netzwerkstruktur – Modus "Transparente Bridge"

Sie müssen wie folgt vorgehen:

- Konfigurieren Sie die Client-Geräte so, dass sie auf das Standard-Gateway verweisen.
- Konfigurieren Sie das Gerät so, dass das Internet-Gateway als Standard-Gateway verwendet wird.
- Stellen Sie sicher, dass Ihre Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.

Modus "Expliziter Proxy"

In diesem Abschnitt lernen Sie den Modus "Expliziter Proxy" des McAfee Email Gateways besser kennen.

Im Modus "Expliziter Proxy" müssen einige Netzwerkgeräte so eingerichtet werden, dass sie Datenverkehr explizit an das Gerät senden. Das Gerät fungiert dann als Proxy oder Relay und verarbeitet den Datenverkehr für die Geräte.

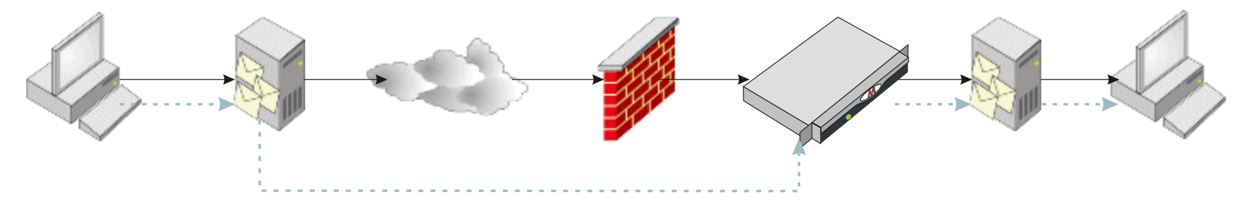


Abbildung 1-5 Modus "Expliziter Proxy" – sichtbarer Datenpfad

Der Modus "Expliziter Proxy" ist am besten für Netzwerke geeignet, in denen Client-Geräte über ein einzelnes Upstream- und Downstream-Gerät eine Verbindung zum Gerät herstellen.



Dies ist möglicherweise nicht die beste Option, wenn verschiedene Netzwerkgeräte erneut konfiguriert werden müssen, damit sie den Datenverkehr an das Gerät senden.

Netzwerk- und Gerätekonfiguration

Wenn sich das Gerät im Modus "Expliziter Proxy" befindet, müssen Sie den internen Mail-Server explizit so konfigurieren, dass er E-Mail-Verkehr an das Gerät sendet. Das Gerät prüft den E-Mail-Verkehr, bevor es ihn im Namen des Absenders an den externen Mail-Server weiterleitet. Der externe E-Mail-Server leitet die E-Mail dann an den Empfänger weiter.

Entsprechend muss das Netzwerk so konfiguriert werden, dass eingehende E-Mail-Nachrichten aus dem Internet nicht dem internen Mail-Server, sondern dem Gerät zugestellt werden.

Das Gerät kann den E-Mail-Verkehr dann prüfen, bevor es ihn im Namen des Absenders an den internen E-Mail-Server zur Zustellung weiterleitet, wie in der Abbildung dargestellt.

Beispielsweise kann ein externer Mail-Server direkt mit dem Gerät kommunizieren, auch wenn der Datenverkehr möglicherweise mehrere Netzwerkserver passiert, bevor er das Gerät erreicht. Der wahrgenommene Pfad verläuft vom externen Mail-Server zum Gerät.

Protokolle

Um ein unterstütztes Protokoll zu scannen, müssen Sie Ihre anderen Netzwerkserver oder Client-Computer so konfigurieren, dass das Protokoll durch das Gerät geleitet wird, sodass kein Datenverkehr das Gerät umgehen kann.

Firewall-Regeln

Im Modus "Expliziter Proxy" werden alle Firewall-Regeln, die für den Client-Zugriff auf das Internet eingerichtet wurden, außer Kraft gesetzt. Für die Firewall sind nur die physischen IP-Adressinformationen für das Gerät sichtbar, nicht jedoch die IP-Adressen der Clients. Die Firewall kann daher ihre Internetzugriffsregeln nicht auf die Clients anwenden.

Stellen Sie sicher, dass die Firewall-Regeln aktualisiert werden. Die Firewall muss den Datenverkehr vom McAfee® Email Gateway akzeptieren, darf aber keinen Datenverkehr verarbeiten, der direkt von den Client-Geräten kommt.

Richten Sie Firewall-Regeln ein, die verhindern, dass unerwünschter Datenverkehr in Ihr Unternehmen gelangt.

Platzieren des Geräts

Konfigurieren Sie die Netzwerkgeräte so, dass der zu scannende Datenverkehr an das McAfee® Email Gateway gesendet wird. Das ist wichtiger als der Standort des McAfee® Email Gateway.

Der Router muss allen Benutzern erlauben, eine Verbindung zum McAfee® Email Gateway herzustellen.

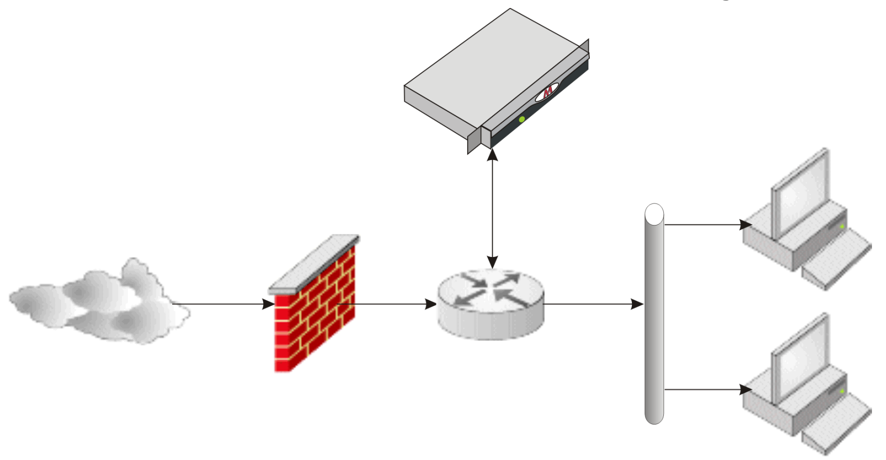


Abbildung 1-6 Platzierung im Modus "Expliziter Proxy"

Das McAfee® Email Gateway muss innerhalb Ihres Unternehmens hinter einer Firewall platziert werden, wie in Abbildung 6 dargestellt: Konfiguration als expliziter Proxy.

Normalerweise ist die Firewall so konfiguriert, dass der Datenverkehr, der nicht direkt von dem Gerät stammt, gesperrt wird. Wenn Sie in Bezug auf die Topologie Ihres Netzwerks unsicher sind und nicht wissen, wie Sie das Gerät integrieren sollen, wenden Sie sich an Ihren Netzwerkspezialisten.

Verwenden Sie diese Konfiguration in folgenden Fällen:

- Das Gerät wird im Modus "Expliziter Proxy" betrieben.
- Sie verwenden E-Mail (SMTP).

Für diese Konfiguration gilt:

- Konfigurieren Sie die externen DNS-Server (Domain Name System) oder NAT (Network Address Translation) auf der Firewall so, dass der externe Mail-Server E-Mails an das Gerät zustellt, nicht an den internen Mail-Server.
- Konfigurieren Sie die internen Mail-Server so, dass E-Mail-Verkehr an das Gerät gesendet wird. Das heißt, die internen Mail-Server müssen das Gerät als Smart-Host verwenden. Vergewissern Sie sich, dass die Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.
- Stellen Sie sicher, dass die Firewall-Regeln aktualisiert werden. Die Firewall muss den Datenverkehr von dem Gerät akzeptieren, darf aber keinen Datenverkehr verarbeiten, der direkt von den Client-Geräten kommt. Richten Sie Regeln ein, die verhindern, dass unerwünschter Datenverkehr in Ihr Unternehmen gelangt.

Ausbringungsstrategien für die Verwendung des Geräts in einer DMZ

Lernen Sie demilitarisierte Zonen in Ihrem Netzwerk kennen, und erfahren Sie, wie Sie diese zum Schutz Ihrer E-Mail-Server verwenden können.

Eine "demilitarisierte Zone" (Demilitarized Zone, DMZ) ist ein Netzwerk, das durch eine Firewall von allen anderen Netzwerken getrennt ist, auch vom Internet und anderen internen Netzwerken. Eine DMZ wird üblicherweise mit dem Ziel implementiert, den Zugriff auf Server zu sperren, die Internetdienste (beispielsweise E-Mail) zur Verfügung stellen.

Hacker verschaffen sich oft Zugriff auf Netzwerke, indem sie herausfinden, auf welchen TCP-/UDP-Ports Appliances Anfragen erwarten, und dann bekannte Schwachstellen in Appliances ausnutzen. Firewalls senken das Risiko solcher Exploits erheblich, indem sie den Zugriff auf bestimmte Ports auf bestimmten Servern steuern.

Das Gerät kann einfach zu einer DMZ-Konfiguration hinzugefügt werden. Die Art, wie Sie das Gerät in einer DMZ verwenden, hängt von den zu scannenden Protokollen ab.

SMTP-Konfiguration in einer DMZ

Erfahren Sie, wie Sie SMTP-Geräte, die sich innerhalb einer demilitarisierten Zone Ihres Netzwerks befinden, konfigurieren.

Die DMZ ist eine gute Möglichkeit für das Verschlüsseln von E-Mails. Wenn der E-Mail-Verkehr die Firewall zum zweiten Mal erreicht (auf seinem Weg von der DMZ zum Internet), ist er verschlüsselt.

Geräte, die SMTP-Verkehr in einer DMZ scannen können, sind normalerweise im Modus "Expliziter Proxy" konfiguriert.

Konfigurationsänderungen müssen nur an den MX-Einträgen für die E-Mail-Server vorgenommen werden.



HINWEIS: Sie können den Modus "Transparente Bridge" verwenden, wenn Sie SMTP in einer DMZ scannen. Wenn Sie jedoch den Datenfluss nicht richtig steuern, scannt das Gerät jede Nachricht zweimal, einmal in jede Richtung. Aus diesem Grund wird für SMTP-Scans normalerweise der Modus "Expliziter Proxy" verwendet.

E-Mail-Relay

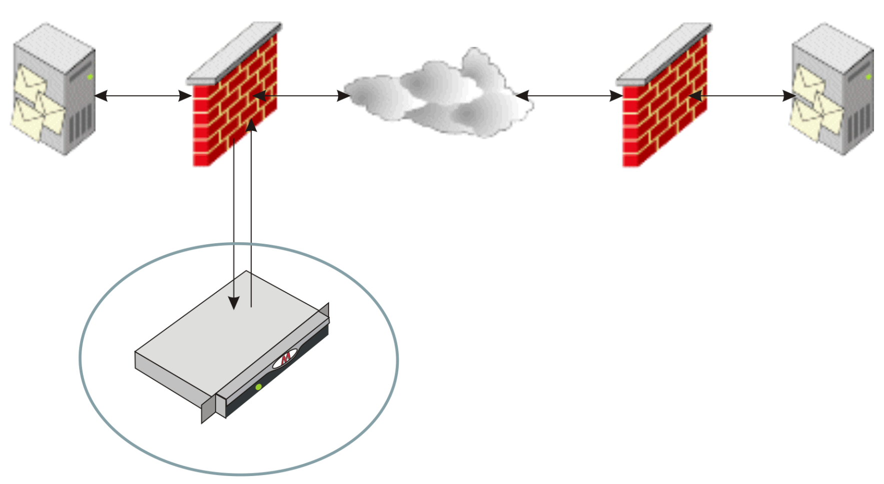


Abbildung 1-7 Konfigurieren als Mail-Relay

Wenn Sie in Ihrer DMZ bereits ein Relay eingerichtet haben, können Sie es durch das Gerät ersetzen.

Um Ihre bestehenden Firewall-Richtlinien zu verwenden, geben Sie dem Gerät dieselbe IP-Adresse wie dem Mail-Relay.

E-Mail-Gateway

SMTP bietet keine Methoden zur Verschlüsselung von E-Mail-Nachrichten. Sie können mithilfe von TLS (Transport Layer Security) den Link verschlüsseln, nicht jedoch die E-Mail-Nachrichten. Daher erlauben einige Unternehmen solchen Datenverkehr nicht in ihrem internen Netzwerk. Zur Umgehung dieses Problems wird häufig ein proprietäres E-Mail-Gateway eingesetzt, zum Beispiel Lotus Notes® oder Microsoft® Exchange, um den E-Mail-Datenverkehr zu verschlüsseln, bevor er das Internet erreicht.

Um eine DMZ-Konfiguration unter Verwendung des proprietären E-Mail-Gateways zu implementieren, fügen Sie das Scan-Gerät zur DMZ auf der SMTP-Seite des Gateways hinzu.

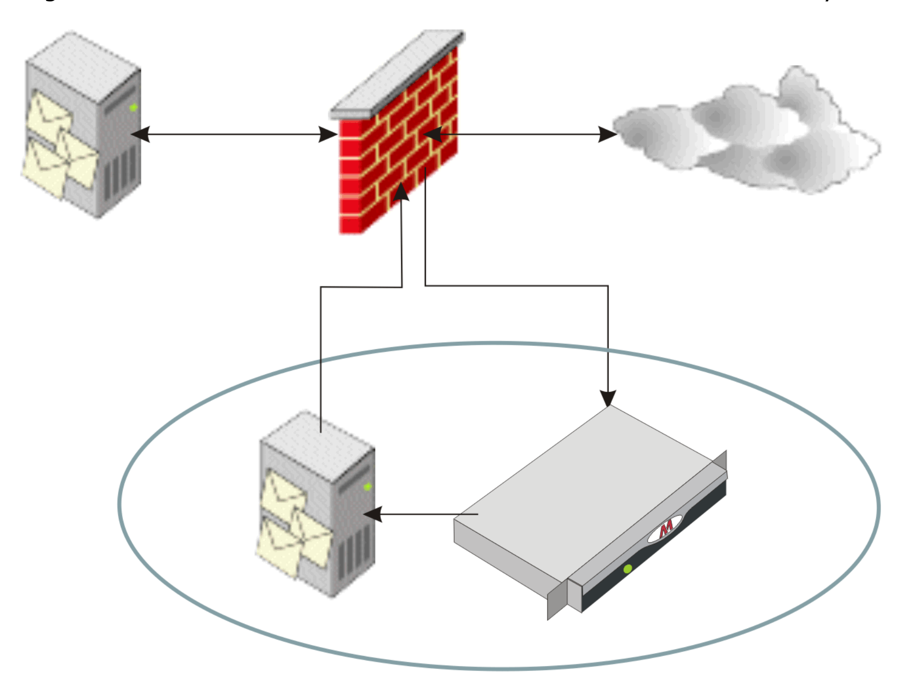


Abbildung 1-8 Konfigurieren als E-Mail-Gateway

Nehmen Sie hierfür folgende Konfigurationen vor:

- Die öffentlichen MX-Einträge müssen externe Mail-Server anweisen, alle eingehenden E-Mail-Nachrichten an das Gerät (statt an das Gateway) zu senden.
- Das Gerät muss alle eingehenden E-Mail-Nachrichten an das Mail-Gateway und alle ausgehenden Nachrichten per DNS oder über ein externes Relay senden.
- Das E-Mail-Gateway muss alle eingehenden E-Mails an die internen Mail-Server und aller andere (ausgehenden) Mails an das Gerät weiterleiten.
- Die Firewall erlaubt nur eingehende E-Mails, die sich an das Gerät richten.



Bei Firewalls, auf denen die Verwendung von NAT (Network Address Translation) konfiguriert ist und die eingehende E-Mails an die internen E-Mail-Server umleiten, müssen die öffentlichen MX-Einträge nicht neu konfiguriert werden. Sie leiten den Datenverkehr bereits an die Firewall und nicht an das eigentliche E-Mail-Gateway. In diesem Fall muss die Firewall neu konfiguriert werden, sodass eingehende Nachrichten an das Gerät geleitet werden.

Für Lotus Notes spezifische Firewall-Regeln

Erfahren Sie, welche speziellen Aspekte beim Schutz von Lotus Notes-Systemen zu berücksichtigen sind.

Lotus Notes-Server kommunizieren standardmäßig über TCP-Port 1352. Die für den Schutz von Notes-Servern in einer DMZ verwendeten Firewall-Regeln erlauben üblicherweise folgendem Datenverkehr das Passieren durch die Firewall:

- Eingehende SMTP-Anforderungen (TCP-Port 25) vom Internet, die für das Gerät bestimmt sind
- Anforderungen auf TCP-Port 1352 aus dem Notes-Gateway, die an einen internen Notes-Server gerichtet sind

- Anforderungen auf TCP-Port 1352 von einem internen Notes-Server, die an das Notes-Gateway gerichtet sind
- SMTP-Anforderungen vom Gerät, die für das Internet bestimmt sind

Alle anderen SMTP-Anforderungen und Anforderungen auf TCP-Port 1352 werden verweigert.

Für Microsoft Exchange spezifische Firewall-Regeln

Erfahren Sie, welche speziellen Aspekte beim Schutz von Microsoft Exchange-Systemen zu berücksichtigen sind.

Ein auf Microsoft Exchange basierendes E-Mail-System erfordert eine erhebliche Umkonfiguration.

Wenn Exchange-Server miteinander kommunizieren, senden sie die ersten Pakete mithilfe des RPC-Protokolls (TCP-Port 135). Sobald die ursprüngliche Kommunikation jedoch eingerichtet ist, werden zwei Ports dynamisch ausgewählt und verwendet, um alle nachfolgenden Pakete für den Rest der Kommunikation zu senden. Sie können die Firewall nicht so konfigurieren, dass sie diese dynamisch gewählten Ports erkennt. Deshalb leitet die Firewall diese Pakete nicht weiter.

Die Ausweichlösung lautet, die Registrierung auf jedem Exchange-Server zu modifizieren, der über die Firewall kommuniziert, sodass immer dieselben zwei "dynamischen" Ports verwendet werden, und dann TCP 135 und diese beiden Ports auf der Firewall zu öffnen.

Wir erwähnen diese Ausweichlösung, um eine umfassende Erklärung zu bieten, wir empfehlen sie jedoch nicht. Das RPC-Protokoll ist in Microsoft-Netzwerken weit verbreitet. Das Öffnen von TCP 135 für eingehenden Datenverkehr ist für die meisten Sicherheitsexperten ein rotes Tuch.

Wenn Sie diese Ausweichlösung verwenden möchten, finden Sie Details im folgenden KnowledgeBase-Artikel auf der Microsoft-Website:

http://support.microsoft.com/kb/q176466/

Arbeitslastverwaltung

In diesem Abschnitt lernen Sie Funktionen zur Arbeitslastverwaltung des McAfee Email Gateways kennen.

Die Appliance verfügt über eine eigene interne Arbeitslastverwaltung, durch die die Scan-Last gleichmäßig auf alle für die Zusammenarbeit konfigurierten Appliances verteilt wird.

Sie müssen kein separates externes Lastausgleichsystem bereitstellen.

2 Installieren der McAfee Email Gateway-Appliance

Lernen Sie den empfohlenen Prozess zum Installieren, Verbinden und Konfigurieren Ihres McAfee Email Gateways kennen.

McAfee empfiehlt, dass Sie bei der Installation des McAfee Email Gateways folgende Reihenfolge einhalten:

1. Entpacken Sie das McAfee Email Gateway, und vergewissern Sie sich, dass keine Teile fehlen (prüfen Sie dies anhand der Teileliste in der Packung).
2. Montieren Sie das McAfee Email Gateway im Rack.
3. Schließen Sie die Peripheriegeräte (Monitor, Tastatur) und die Stromversorgung an.
4. Schließen Sie das McAfee Email Gateway an das Netzwerk an; beachten Sie dabei Ausbringungsszenarien und den gewünschten Netzwerkmodus.
5. Installieren Sie die Software auf dem McAfee Email Gateway.
6. Führen Sie mit der Konfigurationskonsole oder dem Setup-Assistenten die Erstkonfiguration durch (Servername, IP-Adressen, Gateway usw.).
7. Leiten Sie Testnetzwerkverkehr durch das McAfee Email Gateway.
8. Testen Sie, ob der Netzwerkverkehr gescannt wird.
9. Konfigurieren Sie Richtlinien und Berichte.
10. Leiten Sie Produktionsverkehr durch das McAfee Email Gateway.



Beim Anschluss von McAfee Email Gateway an Ihr Netzwerk können Netzwerkdienste unterbrochen werden. Planen Sie einen Zeitraum ein, in dem das Netzwerk nicht verfügbar ist, vorzugsweise zu einer Zeit mit geringer Netzwerkauslastung.

Inhalt

Kurzanleitung für die Installation

Hier erhalten Sie nützliche Informationen zur Reihenfolge der Installation.

1. Packen Sie alle Komponenten aus, und überprüfen Sie den Inhalt anhand der Teilelisten in der Kiste.
2. Schließen Sie die Peripheriegeräte und die Stromversorgung an.
3. Schließen Sie die Appliance an das Netzwerk an.
4. Installieren Sie die Software.
5. Führen Sie die Erstkonfiguration durch (Servername, IP-Adressen, Gateway usw.).
6. Leiten Sie den Testnetzwerkverkehr durch die Appliance.
7. Stellen Sie eine Verbindung zur Benutzeroberfläche her, indem Sie zu https://<ip address>:10443 navigieren.
8. Testen Sie, ob der Netzwerkverkehr gescannt wird.
9. Konfigurieren Sie Richtlinien und die Berichterstellung.
10. Konfigurieren Sie den Produktionsverkehr durch das System.

Anschlüsse und Verbindungen

Informationen über Anschlüsse und Verbindungen sind in diesem Handbuch nicht mehr enthalten.

Weitere Informationen über die Anschlüsse Ihrer Appliance finden Sie in der *Beschreibung der Hardware-Anschlüsse für McAfee Email Gateway*.

Montieren der Appliance

Gehen Sie wie nachfolgend beschrieben vor, um die Appliance mit Ihrem Netzwerk zu verbinden.

Vorgehensweise

1. Nehmen Sie die Appliance aus der Schutzverpackung, und legen Sie sie auf eine ebene Fläche.
2. Wenn Sie die Appliance in einem 19-Zoll-Rack montieren möchten, führen Sie die Schritte unter *Montieren der Appliance in einem Rack* aus.
3. Schließen Sie einen Monitor, eine Tastatur und eine Maus an die Appliance an.
4. Verbinden Sie die Netzkabel mit dem Monitor und der Appliance, schließen Sie sie jedoch noch nicht an die Spannungsversorgung an.
5. Schließen Sie die Appliance unter Beachtung des gewählten Betriebsmodus an das Netzwerk an.

Montieren der Appliance in einem Rack

Erfahren Sie, wie Sie die Appliance in einem Rack montieren.

Das Montage-Set ermöglicht die Installation in einem zweireihigen Rack. Das Montage-Set kann für die meisten 19-Zoll-Racks nach Industriestandard verwendet werden.

Das Montage-Set beinhaltet:

- 2 Halteschienen
- 8 Schrauben
- 2 wiederverwendbare Kabelbinder

Sie benötigen einen für die Schrauben passenden Schraubendreher.



Beachten Sie unbedingt die Sicherheitswarnungen. Beladen Sie das Rack immer von unten nach oben. Wenn Sie mehrere Appliances installieren, sollten Sie mit der untersten freien Stelle beginnen.

Verbindung mit dem Netzwerk

Erfahren Sie, wie Sie Ihr McAfee Email Gateway mit Ihrem Netzwerk verbinden.

In diesem Abschnitt wird erläutert, wie die Appliance an Ihr Netzwerk angeschlossen wird.

Welche Anschlüsse und Kabel Sie dazu verwenden, hängt vom Betriebsmodus der Appliance ab. Weitere Informationen über Netzwerkmodi finden Sie unter *Überlegungen zu Netzwerkmodi*.

Port-Nummern

Lernen Sie einige der wichtigen Ports kennen, die von der Appliance verwendet werden.

Verwenden Sie die folgenden Port-Nummern, wenn Sie die Appliance mit Ihrem Netzwerk verbinden:

- Verwenden Sie Port 443 für HTTPS.
- Verwenden Sie Port 80 für HTTP.
- Verwenden Sie Port 25 für SMTP.
- Verwenden Sie Port 110 für POP3.
- Verwenden Sie Port 21 für FTP.

Verwenden von Kupfer-LAN-Verbindungen

Erfahren Sie, wie Sie Ihr McAfee Email Gateway über Kupferkabel an Ihr Netzwerk anschließen.

Verwenden Sie die LAN1- und LAN2-Switch-Verbindungen und die im Lieferumfang enthaltenen Netzwerkkabel (oder entsprechende Cat-5e- bzw. Cat-6-Ethernet-Kabel), und schließen Sie die Appliance entsprechend dem gewählten Netzwerkmodus an Ihr Netzwerk an.

Falls Sie in Ihrem Netzwerk DHCP konfiguriert haben, werden die IP-Adressen für diese Anschlüsse jetzt automatisch zugewiesen.

Modus "Transparente Bridge"

Schließen Sie die LAN1- und LAN2-Switches des E-Mail-Gateways mit den mitgelieferten Kupfer-LAN-Kabeln an Ihr Netzwerk an, um die Appliance in den Datenstrom einzufügen.

Modus "Transparenter Router"

Das E-Mail-Gateway fungiert als Router. Die LAN-Segmente, die mit den beiden Netzwerkschnittstellen verbunden sind, müssen sich deshalb in verschiedenen IP-Subnetzen befinden. Sie muss einen bestehenden Router ersetzen, oder auf der Seite der Appliance muss ein neues Subnetz angelegt werden. Ändern Sie hierfür die IP-Adresse oder die Netzmaske, die die Computer auf dieser Seite verwenden.

Modus "Expliziter Proxy"

Schließen Sie den LAN1- oder LAN2-Switch mit einem Kupfer-LAN-Kabel (mitgeliefert) an das Netzwerk an. Bei diesem Kabel handelt es sich um ein durchgängiges (ungekreuztes) Kabel, das die Appliance mit einem normalen, ungekreuzten RJ-45-Netzwerk-Switch verbindet.

Im Modus "Expliziter Proxy" kann die nicht verwendete Switch-Verbindung als dedizierter Management-Port verwendet werden. Um die Appliance lokal verwalten zu können, schließen Sie die Appliance über ein gekreuztes Cat-5e-Ethernet-Kabel an die Netzwerkkarte des lokalen Computers an.

Verwenden von Glasfaser-LAN-Verbindungen

Erfahren Sie, wie Sie Ihr McAfee Email Gateway über Glasfaseroptikverbindungen an Ihr Netzwerk anschließen.

Verwenden Sie die LAN1- und LAN2-Switch-Verbindungen und die Glasfaserkabel, und schließen Sie die Appliance entsprechend dem gewählten Netzwerkmodus an Ihr Netzwerk an.

Modus "Transparente Bridge"

Schließen Sie die LAN1- und LAN2-Switches mit Glasfaserkabeln an das Netzwerk an.

Modus "Transparenter Router"

Schließen Sie die LAN1- und LAN2-Switches mit Glasfaserkabeln an verschiedene IP-Subnetze an.

Modus "Expliziter Proxy"

Schließen Sie den LAN1-Switch der Appliance mit einem Glasfaserkabel an das Netzwerk an.

Im Modus "Expliziter Proxy" kann der nicht verwendete Konnektor als dedizierter Management-Port verwendet werden. Wenn der Verwaltungscomputer über eine kompatible Netzwerkkarte verfügt, schließen Sie ihn zur lokalen Verwaltung an den verbleibenden Konnektor an.

Monitor, Maus und Tastatur

In diesem Abschnitt erfahren Sie, wie Sie einen Computer-Monitor, eine Maus und eine Tastatur an Ihr McAfee Email Gateway anschließen.

Schließen Sie einen Computer-Monitor an den VGA-Anschluss Ihres McAfee Email Gateways an.

Schließen Sie die Tastatur und die Maus an die USB-Anschlüsse des McAfee Email Gateways an.

Anschließen der Appliance an das Stromnetz

Gehen Sie wie nachfolgend beschrieben vor, um die Appliance an das Stromnetz anzuschließen und einzuschalten.

Vorgehensweise

1. Schließen Sie die Netzkabel der Appliance und des Monitors an die Stromsteckdosen an.

   Falls das Netzkabel für das Einsatzland nicht geeignet ist, setzen Sie sich mit Ihrem Händler in Verbindung.

2. Schalten Sie die Appliance ein, indem Sie den Netzschalter drücken.

   Nach dem Hochfahren wird die Konfigurationskonsole auf dem Monitor angezeigt.

Installieren der Software

Ein Überblick über den Software-Installationsvorgang für McAfee® Email Gateway.

Vorgehensweise

1. Laden Sie von einem Computer mit Internetzugang aus die neueste Version des McAfee® Email Gateway von der McAfee-Download-Seite herunter. (Sie benötigen hierfür Ihre Grant-Nummer.)
2. Erstellen Sie von diesem Image eine CD.
3. Schalten Sie das Gerät ein, und legen Sie die CD in das CD-ROM-Laufwerk ein.
4. Starten Sie das Gerät neu.

   Wenn das McAfee® Email Gateway neu startet, wird die Software auf dem Gerät installiert.

Aufgaben

- *Vorgehensweise – Herunterladen der Installations-Software* auf Seite 25
  Gehen Sie wie nachfolgend beschrieben vor, um die aktuellste Version der McAfee Email Gateway-Software herunterzuladen.
- *Vorgehensweise – Erstellen einer CD anhand des Installations-Software-Images* auf Seite 26
  Gehen Sie wie nachfolgend beschrieben vor, um eine Installations-CD anhand des heruntergeladenen Software-Images zu erstellen.

Vorgehensweise – Herunterladen der Installations-Software

Gehen Sie wie nachfolgend beschrieben vor, um die aktuellste Version der McAfee Email Gateway-Software herunterzuladen.

Bevor Sie beginnen

- Lesen Sie das Installationshandbuch zu Ihrem -Produkt.
- Suchen Sie nach der McAfee-Grant-Nummer, die Sie beim Kauf von McAfee Email Gateway erhalten haben.

McAfee bietet die Software auf der McAfee-Download-Website als ISO-Datei an (zum Erstellen von Installations-CDs für physische Appliances).

Vorgehensweise

1. Besuchen Sie die McAfee-Website http://www.mcafee.com. Halten Sie den Mauszeiger über Ihren Geschäftstyp, und klicken Sie auf **Downloads**.
2. Klicken Sie auf der Seite **Meine Produkte – Downloads** auf **Anmelden**.
3. Geben Sie die McAfee-Grant-Nummer ein, die Sie beim Kauf von McAfee Email Gateway erhalten haben, und klicken Sie auf **Senden**.
4. Wählen Sie aus der Produktliste **Email Gateway** aus.
5. Akzeptieren Sie die Lizenzbedingungen, wählen Sie die neueste Version, und laden Sie sie herunter.



McAfee empfiehlt, dass Sie die Versionsinformationen lesen, die Sie mit dem Software-Image erhalten, bevor Sie die Installation fortsetzen.

Vorgehensweise – Erstellen einer CD anhand des Installations-Software-Images

Gehen Sie wie nachfolgend beschrieben vor, um eine Installations-CD anhand des heruntergeladenen Software-Images zu erstellen.

Bevor Sie beginnen

- Laden Sie das Software-Image als ISO-Datei herunter.
- Stellen Sie sicher, dass Sie die heruntergeladene ISO-Datei durch Vergleichen der MD5-Prüfsummen validieren können.
- Sie benötigen an Ihrem Computer-System einen geeigneten CD-Brenner sowie geeignete CDs.
- Weiterhin muss auf Ihrem Computer eine geeignete CD-Brenn-Software installiert sein, die eine CD anhand einer ISO-Datei erstellen kann.

Führen Sie auf einem Computer, der Zugriff auf das heruntergeladene ISO-Image hat, folgende Schritte durch.

Vorgehensweise

1. Validieren Sie die heruntergeladene ISO-Datei, indem Sie eine MD5-Prüfsumme generieren und diese mit dem Wert vergleichen, der auf der Download-Seite angegeben ist.
2. Folgen Sie den zu Ihrer CD-Brenn-Software gehörigen Anweisungen, und öffnen Sie die Software.
3. Wählen Sie gemäß dem Workflow Ihrer CD-Brenn-Software den CD-Brenner und die ISO-Datei von McAfee Email Gateway aus. Legen Sie eine leere beschreibbare CD in das Laufwerk ein.
4. Erstellen Sie die Installations-CD.

Verwenden der Konfigurationskonsole

Erfahren Sie, wie Sie das McAfee Email Gateway mithilfe der Konfigurationskonsole einrichten.

Sie können Ihr McAfee Email Gateway entweder von der Konfigurationskonsole aus oder innerhalb der Benutzeroberfläche mit dem Setup-Assistenten konfigurieren.

Die Konfigurationskonsole wird am Ende der Startsequenz automatisch gestartet, entweder nachdem:

- ein nicht konfiguriertes McAfee Email Gateway gestartet wurde,
- oder nachdem ein McAfee Email Gateway auf die Werkseinstellungen zurückgesetzt wurde.

Nach dem Start bietet Ihnen die **Konfigurationskonsole** Optionen, um Ihr Gerät von der McAfee Email Gateway-Konsole aus in Ihrer bevorzugten Sprache zu konfigurieren, bzw. liefert Anweisungen dafür, wie Sie von einem anderen Computer im selben Klasse-C-Subnetz (/24) aus eine Verbindung mit dem **Setup-Assistenten** innerhalb der Benutzeroberfläche herstellen können. Beide Methoden bieten Ihnen dieselben Optionen für die Konfiguration Ihres McAfee Email Gateway.



Von der **Konfigurationskonsole** aus können Sie eine neue Installation der Appliance-Software konfigurieren. Wenn Sie jedoch für die Konfiguration Ihrer Appliance eine zuvor gespeicherte Konfigurationsdatei verwenden möchten, müssen Sie sich bei der Benutzeroberfläche der Appliance anmelden und den Setup-Assistenten ausführen (**System | Setup-Assistent**).

Ebenso wird mit dieser Softwareversion für folgende Parameter die automatische Konfiguration mithilfe von DHCP eingeführt:

- Host-Name
- Domänenname
- Standard-Gateway
- DNS-Server
- Geleaste IP-Adresse
- NTP-Server

Weitere Informationen zu jeder Seite der **Konfigurationskonsole** und des **Setup-Assistenten** erhalten Sie auf dem Bildschirm.

Durchführen der Standardeinrichtung

In diesem Abschnitt erfahren Sie, welchen Zweck die Standardeinrichtung hat.

Die **Standardeinrichtung** ermöglicht Ihnen die schnelle Einrichtung Ihres McAfee Email Gateways unter Verwendung der gängigsten Optionen. Verwenden Sie diese Option, um das Gerät im Modus "Transparente Bridge" einzurichten und für den Schutz Ihres Netzwerks zu konfigurieren. Das SMTP-Protokoll ist standardmäßig aktiviert. Sie können wählen, ob POP3-Verkehr gescannt werden soll.



Mit der Wahl der **Standardeinrichtung** wird für das Gerät der Modus "Transparente Bridge" erzwungen.

Bei der **Standardeinrichtung** enthält der Assistent die folgenden Seiten:

- **E-Mail-Konfiguration**
- **Grundlegende Einstellungen**
- **Zusammenfassung**

Durchführen der benutzerdefinierten Einrichtung

In diesem Abschnitt erfahren Sie, welchen Zweck die benutzerdefinierte Einrichtung hat.

Die **Benutzerdefinierte Einrichtung** ermöglicht Ihnen eine größere Kontrolle über die Optionen, die Sie auswählen können, darunter den Betriebsmodus des Geräts. Sie können auswählen, dass der E-Mail-Verkehr über die Protokolle SMTP und POP3 geschützt wird. Verwenden Sie diese Konfigurationsoption, um IPv6 zu konfigurieren und sonstige Änderungen an der Standardkonfiguration vorzunehmen.

Bei der **Benutzerdefinierten Einrichtung** enthält der Assistent die folgenden Seiten:

- **E-Mail-Konfiguration**
- **Grundlegende Einstellungen**
- **Netzwerkeinstellungen**
- **Cluster-Verwaltung**
- **DNS und Routing**
- **Zeiteinstellungen**
- **Kennwort**
- **Zusammenfassung**

Wiederherstellung aus einer Datei

In diesem Abschnitt erfahren Sie, welchen Zweck die Wiederherstellung aus einer Datei hat.

Wenn Sie Ihr Gerät über den **Setup-Assistenten** innerhalb der Benutzeroberfläche konfigurieren, können Sie mithilfe der Option **Aus Datei wiederherstellen** zuvor gespeicherte Konfigurationsdaten importieren und auf Ihr Gerät übernehmen. Nachdem diese Daten importiert wurden, können Sie Änderungen vornehmen, bevor Sie die Konfiguration anwenden.



Die Option **Aus Datei wiederherstellen** ist in der **Konfigurationskonsole** nicht verfügbar. Zum Verwenden dieser Option müssen Sie sich beim McAfee Email Gateway anmelden und **Aus Datei wiederherstellen** aus dem Menü **System | Setup-Assistent** auswählen.

Nachdem die Konfigurationsdaten importiert wurden, werden die Optionen der **Benutzerdefinierten Einrichtung** im **Setup-Assistenten** angezeigt (siehe *Durchführen der benutzerdefinierten Einrichtung*). Alle importierten Optionen werden auf den Assistentenseiten angezeigt, sodass Sie die Möglichkeit zum Vornehmen von Änderungen haben, bevor Sie die Konfiguration übernehmen.

Bei Verwendung der Option **Aus Datei wiederherstellen** enthält der Assistent die folgenden Seiten:

- **Konfigurationsdatei importieren**
- **Wiederherzustellende Werte**

Nachdem diese Informationen geladen wurden, werden die Seiten der **Benutzerdefinierten Einrichtung** angezeigt, in denen Sie weitere Änderungen vornehmen können, bevor Sie die neue Konfiguration übernehmen:

- **E-Mail-Konfiguration**
- **Grundlegende Einstellungen**
- **Netzwerkeinstellungen**
- **Cluster-Verwaltung**
- **DNS und Routing**
- **Zeiteinstellungen**
- **Kennwort**
- **Zusammenfassung**

Einrichten der Verwaltung durch ePolicy Orchestrator

In diesem Abschnitt erfahren Sie, welchen Zweck die Option **Einrichten der Verwaltung durch ePolicy Orchestrator** hat.

McAfee ePolicy Orchestrator ermöglicht Ihnen, Ihre gesamten McAfee®-Software- und Hardware-Appliances von einer einzelnen Verwaltungskonsole aus zu verwalten.

Mit dem Assistenten **Einrichten der Verwaltung durch ePolicy Orchestrator** können Sie Ihr Gerät so konfigurieren, dass es von Ihrem McAfee ePolicy Orchestrator-Server aus verwaltet werden kann.

Es wird nur ein Minimum an Informationen benötigt, da das Gerät die meisten Konfigurationsdaten von Ihrem McAfee ePolicy Orchestrator-Server erhält.

Einstellungen für die ePolicy Orchestrator-Verwaltung

Wählen Sie „Einrichten der Verwaltung durch ePolicy Orchestrator" im Setup-Assistenten, um die Appliance für die Verwaltung durch McAfee ePolicy Orchestrator zu konfigurieren.

Option	Beschreibung
ePO-Erweiterungen	Laden Sie die McAfee ePolicy Orchestrator-Erweiterungen für McAfee Gateway-Produkte herunter, einschließlich McAfee Email Gateway. Die Datei *MEGv7.x_ePOextensions.zip* enthält sowohl die EWG- als auch die MEG McAfee ePolicy Orchestrator-Erweiterungen. Die EWG-Erweiterung ermöglicht die Berichterstellung von McAfee ePolicy Orchestrator aus für die folgenden Produkte: • McAfee Email and Web Security-Appliances • McAfee Web Gateway-Appliances • McAfee E-Mail Gateway-Appliances Die MEG-Erweiterung bietet eine vollständige McAfee ePolicy Orchestrator-Verwaltung für McAfee Email Gateway Versionen 7.0 oder höher. Damit Sie McAfee ePolicy Orchestrator für die Berichterstellung oder Verwaltung verwenden können, müssen die McAfee ePolicy Orchestrator-Erweiterungen auf Ihrem McAfee ePolicy Orchestrator-Server installiert sein.
ePO-Hilfe-Erweiterungen	Laden Sie die McAfee ePolicy Orchestrator-Hilfe-Erweiterungen herunter. Die Datei *MEGv7.x_ePOhelpextensions.zip* enthält die Informationen zur Online-Hilfe für die obigen McAfee ePolicy Orchestrator-Erweiterungen. Diese Datei installiert die zu den McAfee ePolicy Orchestrator-Erweiterungen für McAfee Email and Web Gateway sowie McAfee Email Gateway Appliances gehörenden Hilfe-Erweiterungen auf Ihrem McAfee ePolicy Orchestrator-Server.
ePO-Verbindungseinstellungen importieren	Klicken Sie hier, um zur Datei mit den Verbindungseinstellungen für McAfee ePolicy Orchestrator zu navigieren und die McAfee ePolicy Orchestrator-Verbindungsinformationen in die Appliance zu importieren.

Vorgehensweise – Konfigurieren der Appliance für das Arbeiten mit ePolicy Orchestrator

Richten Sie anhand dieser Vorgehensweise die Appliance für die Verwaltung durch ePolicy Orchestrator ein:

1. Wählen Sie auf dem McAfee Email Gateway unter **Einstellungen für die ePO-Verwaltung** die Option **ePO-Erweiterungen**, und klicken Sie auf **Speichern**, um die Erweiterungsdatei herunterzuladen.
2. Wählen Sie auf dem McAfee Email Gateway unter **Einstellungen für die ePO-Verwaltung** die Option **ePO-Hilfe-Erweiterungen**, und klicken Sie auf **Speichern**, um die Hilfe-Erweiterungsdatei herunterzuladen.
3. Installieren Sie diese Erweiterungen auf Ihrem McAfee ePolicy Orchestrator-Server, indem Sie **Menü** | **Software** | **Erweiterungen** | **Erweiterungen installieren** wählen.
4. Speichern Sie auf dem McAfee ePolicy Orchestrator-Server die Verbindungseinstellungen mithilfe des Befehls **Menü** | **Gateway-Schutz** | **E-Mail- und Web-Gateway** | **Aktionen** | **Verbindungseinstellungen exportieren**.

5. Kehren Sie auf dem McAfee Email Gateway auf die Seite **Einstellungen für die ePO-Verwaltung** im **Setup-Assistenten** zurück, und klicken Sie auf **ePO-Verbindungseinstellungen importieren**. Navigieren Sie zur McAfee ePolicy Orchestrator-Verbindungseinstellungsdatei.
6. Klicken Sie auf **Weiter**, um auf der Seite **Grundlegende Einstellungen** im **Setup-Assistenten** fortzufahren.

Setup im Modus 'Nur Verschlüsselung'

In diesem Abschnitt erfahren Sie, welchen Zweck die Einrichtungsoptionen im Modus "Nur Verschlüsselung" haben.

In kleinen bis mittleren Organisationen ist es häufig ausreichend, dasselbe McAfee Email Gateway für E-Mail-Scan- und E-Mail-Verschlüsselungs-Tasks zu verwenden.

Wenn Sie jedoch in einem größeren Unternehmen bzw. in einer Branche arbeiten, in der die Zustellung des gesamten oder eines überwiegenden Teils des E-Mail-Aufkommens auf eine sichere Weise erfolgen muss, kann es empfehlenswert sein, eine oder mehrere McAfee Email Gateway Appliances als eigenständige Verschlüsselungs-Server einzurichten.

Unter diesen Umständen bieten Ihnen die Optionen für das **Setup im Modus "Nur Verschlüsselung"** innerhalb des **Setup-Assistenten** die relevanten Einstellungen, die für den Betrieb im Modus "Nur Verschlüsselung" erforderlich sind.

3 Vorstellung des Dashboards

In diesem Abschnitt wird die Seite **Dashboard** beschrieben und erläutert, wie ihre Voreinstellungen bearbeitet werden.

Das Dashboard

Das **Dashboard** bietet eine Zusammenfassung der Aktivitäten der Appliance.


Dashboard

Von dieser Seite aus können Sie auf die meisten Seiten zugreifen, die die Appliance steuern.

Auf einer Cluster-Master-Appliance verwenden Sie diese Seite auch, um eine Übersicht der Aktivitäten im Appliance-Cluster anzuzeigen.

Vorteile der Verwendung des Dashboards

Das **Dashboard** bietet einen zentralen Ort, an dem Sie Zusammenfassungen der Appliance-Aktivitäten mithilfe verschiedener Portlets ansehen können.

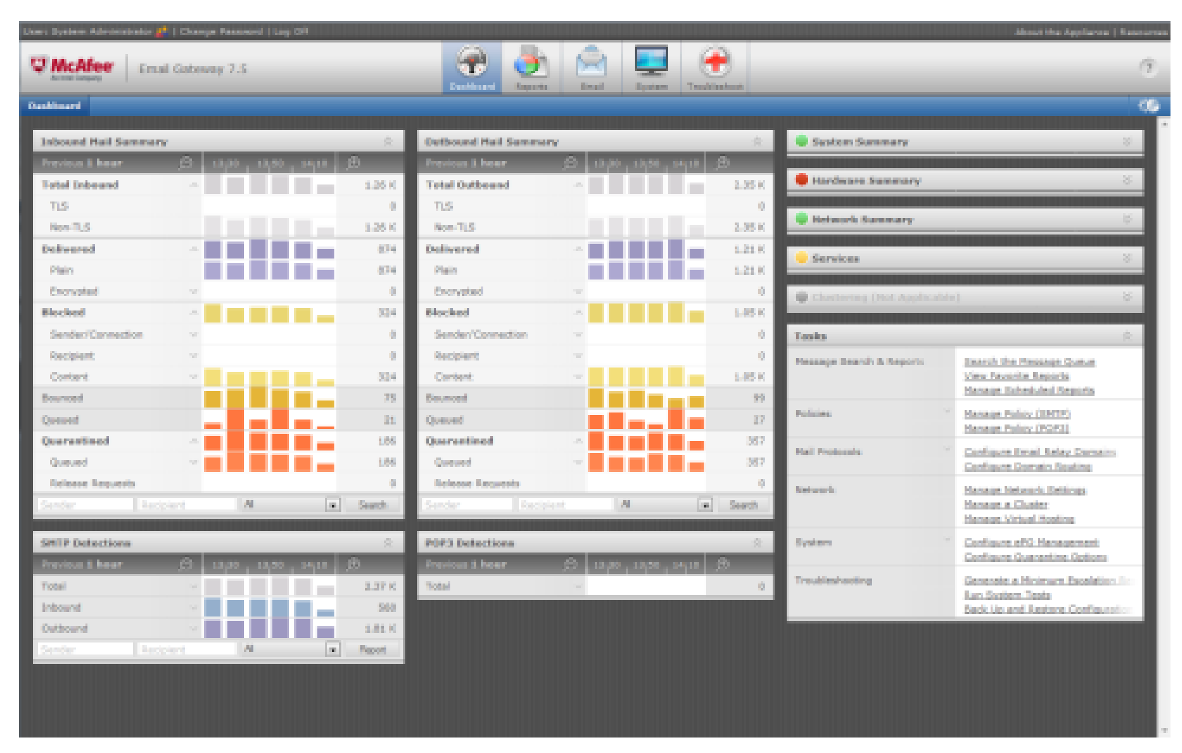


Abbildung 3-1 Dashboard-Portlets

In einigen Portlets werden Grafiken angezeigt, die die Appliance-Aktivität in den folgenden Zeiträumen darstellen:

- 1 Stunde
- 1 Tag (Standard)
- 1 Woche
- 2 Wochen
- 4 Wochen

Im **Dashboard** können Sie einige Änderungen an den angezeigten Informationen und Diagrammen vornehmen:

- Vergrößern und verkleinern Sie die Portlet-Daten mithilfe der Schaltflächen und rechts oben im Portlet.
- Zeigen Sie mithilfe der Schaltflächen und detailliertere Daten an.
- Eine Statusanzeige gibt an, ob das Element Aufmerksamkeit erfordert:
  - **Fehlerfrei**: Die ausgewiesenen Elemente funktionieren normal.
  - **Erfordert Aufmerksamkeit**: Ein Warnungsschwellenwert wurde überschritten.
  - **Erfordert sofortige Aufmerksamkeit**: Ein kritischer Schwellenwert wurde überschritten.
  - **Deaktiviert**: Der Dienst ist nicht aktiviert.

- Verwenden Sie und , um auf einer Zeitachse in Informationen herein- und herauszuzoomen. Es kommt zu einer kurzen Verzögerung, während die Ansicht aktualisiert wird. Standardmäßig zeigt das **Dashboard** Daten für den vorherigen Tag an.
- Verschieben Sie ein Portlet an eine andere Stelle auf dem **Dashboard**.
- Doppelklicken Sie auf die obere Leiste eines Portlets, um es auf den oberen Bereich des **Dashboards** zu vergrößern.
- Legen Sie eigene Warnhinweis- und Warnungsschwellenwerte zum Auslösen von Ereignissen fest. Markieren Sie dazu das Element, und klicken Sie darauf, bearbeiten Sie die Felder "Warnhinweisschwellenwert" und "Warnungsschwellenwert", und klicken Sie auf **Speichern**. Wenn das Element den von Ihnen festgelegten Schwellenwert überschreitet, wird ein Ereignis ausgelöst.



Abhängig von dem Browser, der zum Anzeigen der Benutzeroberfläche von McAfee Email Gateway verwendet wird, speichert das **Dashboard** den aktuellen Status jedes Portlets (ob es vergrößert oder verkleinert ist und ob Sie die Anzeige bestimmter Daten geöffnet haben) und versucht, die entsprechende Ansicht wiederherzustellen, wenn Sie zu einer anderen Seite in der Benutzeroberfläche navigieren und anschließend innerhalb derselben Browsersitzung zum **Dashboard** zurückkehren.

Dashboard-Portlets

Lernen Sie die Portlets auf dem Dashboard der Benutzeroberfläche von McAfee Email Gateway kennen.

Option	Beschreibung
Zusammenfassung der eingehenden E-Mails	Mit dem Portlet **Zusammenfassung der eingehenden E-Mails** können Sie Zustell- und Statusinformationen über Nachrichten abrufen, die an Ihr Unternehmen gesendet wurden.
Zusammenfassung der ausgehenden E-Mails	Mit dem Portlet **Zusammenfassung der ausgehenden E-Mails** können Sie Zustell- und Statusinformationen über Nachrichten abrufen, die von Ihrem Unternehmen aus gesendet wurden.
SMTP-Entdeckungen	Mit dem Portlet **SMTP-Entdeckungen** können Sie die Gesamtanzahl der Nachrichten feststellen, die eine Entdeckung basierend auf Absender, Verbindung, Empfänger oder Inhalt ausgelöst haben, bzw. Daten zum eingehenden oder ausgehenden SMTP-Datenverkehr anzeigen.
POP3-Entdeckungen	Mit dem Portlet **POP3-Entdeckungen** können Sie anzeigen, wie viele Nachrichten eine Entdeckung basierend auf Bedrohungen wie Viren, Komprimierungsprogrammen oder potenziell anstößigen Bildern ausgelöst haben.
Systemzusammenfassung	Mit dem Portlet **Systemzusammenfassung** können Sie Informationen über den Lastausgleich, den für jede Partition verwendeten Speicherplatz, die gesamte CPU-Auslastung, den verwendeten und verfügbaren Arbeitsspeicher sowie Swap-Details anzeigen.
Hardware-Zusammenfassung	Das Portlet **Hardware-Zusammenfassung** verwendet Statusindikatoren, um den Status von Netzwerkschnittstellen, USV-Servern, des Bridge-Modus (sofern aktiviert) sowie den RAID-Status anzuzeigen.
Netzwerkzusammenfassung	Mit dem Portlet **Netzwerkzusammenfassung** können Sie Informationen über den Status Ihrer Verbindungen, den Netzwerkdurchsatz und Zähler in Bezug auf die Kernel-Modus-Blockierung anzeigen.
Dienste	Mit dem Portlet **Dienste** können Sie Statistiken zum Aktualisierungs- und Dienststatus anzeigen, die auf den von der Appliance verwendeten Protokoll- und externen Servern basieren.

Option	Beschreibung
Clustering	Mit dem Portlet **Clustering** können Sie nach der Konfiguration Ihrer Appliance als Bestandteil eines Clusters oder bei Verwendung der Blade-Server-Hardware Informationen über den gesamten Cluster bereitstellen.
Tasks	Mit dem Portlet **Tasks** gelangen Sie direkt zu den Bereichen der Benutzeroberfläche, in denen Sie die Nachrichtenwarteschlange durchsuchen, Berichte anzeigen, Richtlinien verwalten, E-Mail-Protokoll-, Netzwerk- und System-Einstellungen konfigurieren und auf Funktionen zur Fehlerbehebung zugreifen können.

4 Testen der Konfiguration

Diese Informationen beschreiben, wie Sie testen können, ob die Appliance nach der Installation ordnungsgemäß funktioniert.

Inhalt

Vorgehensweise – Testen der Verbindung

Gehen Sie wie nachfolgend beschrieben vor, um die grundlegende Verbindungsfähigkeit zu bestätigen.

Das McAfee Email Gateway prüft, ob es mit dem Gateway kommunizieren und Server sowie DNS-Server aktualisieren kann. Außerdem wird überprüft, ob der Name der Appliance und der Name der Domäne gültig sind.

Vorgehensweise

1. Wählen Sie in der Navigationsleiste die Option **Fehlerbehebung**, oder wählen Sie im Dashboard im Bereich **Tasks** die Option **Systemtests ausführen**.
2. Klicken Sie auf die Registerkarte **Tests**.
3. Klicken Sie auf **Tests starten**.

Jeder Test sollte positiv beendet werden.

Vorgehensweise – Die DAT-Dateien aktualisieren

Gehen Sie wie nachfolgend beschrieben vor, um sicherzustellen, dass das McAfee Email Gateway über die aktuellsten Erkennungsdefinitionsdateien (DAT) verfügt. Es wird empfohlen, dass Sie diese aktualisieren, bevor Sie die Scan-Optionen konfigurieren.

Im Rahmen der Verwendung des McAfee Email Gateway können Sie einzelne Arten von Definitionsdateien aktualisieren sowie die standardmäßig geplanten Aktualisierungen an Ihre Anforderungen anpassen.

Vorgehensweise

1 Wählen Sie **System** | **Komponentenverwaltung** | **Aktualisierungsstatus**.

2 Klicken Sie zum Aktualisieren des Antiviren-Moduls und der Antiviren-Datenbank auf **Jetzt aktualisieren**.

   Für die Überprüfung, ob das Update korrekt angewendet wurde, öffnen Sie das Portlet **Dienste** im Dashboard, und erweitern Sie den Status für **Aktualisierungen**. Die Antiviren-Komponenten haben einen grünen Status.

Vorgehensweise – Testen von E-Mail-Verkehr und Virenerkennung

Gehen Sie wie nachfolgend beschrieben vor, um zu überprüfen, ob der E-Mail-Verkehr erfolgreich durch das McAfee Email Gateway geleitet wird und ob dabei Gefahren ordnungsgemäß identifiziert werden. Wir verwenden die EICAR-Testdatei, eine harmlose Datei, die eine Virenerkennung auslöst.

Vorgehensweise

1 Senden Sie eine E-Mail von einem externen E-Mail-Konto (wie Hotmail) an einen internen Posteingang, und vergewissern Sie sich, dass die E-Mail angekommen ist.

2 Sehen Sie sich im Dashboard die Bereiche mit den Erkennungen an. Aus der Liste für das Protokoll, das Sie zum Versenden der Nachricht verwendet haben, sollte hervorgehen, dass eine Nachricht empfangen wurde.

3 Kopieren Sie die folgende Zeile in eine Datei, und achten Sie dabei darauf, dass Sie keine Leerzeichen oder Zeilenumbrüche hinzufügen:

   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

4 Speichern Sie die Datei unter dem Namen EICAR.COM.

   Abhängig von Ihrer lokalen Antiviren-Software und -Konfiguration kann dies zu einer Entdeckung und Isolierung auf Ihrem lokalen Rechner führen.

5 Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine Nachricht mit der Datei EICAR.COM als Anhang, und senden Sie die Nachricht an einen internen Posteingang.

6 Kehren Sie zum Dashboard zurück, und sehen Sie sich die Bereiche mit den Erkennungen an. Sie sollten sehen, dass ein Virus erkannt wurde.

7 Löschen Sie die Nachricht, wenn Sie das Testen Ihrer Installation abgeschlossen haben, damit ahnungslose Benutzer keinen Schreck bekommen.

Vorgehensweise – Testen der Spam-Erkennung

Gehen Sie wie nachfolgend beschrieben vor, um einen *General Test mail for Unsolicited Bulk Email* (Allgemeiner Test auf unerwünschte Bulk-E-Mails, GTUBE) auszuführen, mit dem geprüft wird, ob das McAfee Email Gateway eingehende Spam-Mail erkennt.

Vorgehensweise

1. Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine neue E-Mail.
2. Kopieren Sie den folgenden Text in den Nachrichtenteil der E-Mail:

   XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

   Achten Sie darauf, dass der Text keine Zeilenumbrüche enthält.
3. Senden Sie die neue E-Mail an eine interne Posteingangsadresse.

   Das Gerät scannt die Nachricht, erkennt sie als Junk-E-Mail und verarbeitet sie entsprechend. Der GTUBE-Test hat Vorrang vor Blacklists und Whitelists.

   Nähere Informationen zum GTUBE-Test finden Sie unter http://spamassassin.apache.org/tests.html.

5 Erkunden der Funktionen der Appliance

Diese Informationen enthalten Vorgehensweisen zur Demonstration der ausgeführten Scan-Funktionen von McAfee Email Gateway. Sie werden detailliert durch das Erstellen und Testen einiger Beispielrichtlinien geführt und erfahren, wie Sie die relevanten Berichte generieren.

Einführung in die Richtlinien

Die Appliance verwendet Richtlinien zur Beschreibung der Aktionen, die die Appliance bei Bedrohung durch Viren, Spam, unerwünschte Dateien und Verlust kritischer Informationen ausführen muss.



Email | Email Policies

Richtlinien sind Sammlungen von Regeln oder Einstellungen, die auf bestimmte Arten von Datenverkehr oder auf Benutzergruppen angewendet werden können.

Verschlüsselung

Auf den Seiten **Verschlüsselung** können Sie McAfee Email Gateway für die Verwendung unterstützter Verschlüsselungsverfahren konfigurieren, damit E-Mail-Nachrichten sicher zugestellt werden.



E-Mail | Verschlüsselung

Das McAfee Email Gateway umfasst mehrere Verschlüsselungs-Methoden und kann dafür eingerichtet werden, anderen Scan-Funktionen Verschlüsselungsdienste zur Verfügung zu stellen. Es kann jedoch auch als reiner Verschlüsselung-Server nur für die Verschlüsselung von E-Mails verwendet werden.

Vorgehensweise – Verschlüsseln des gesamten E-Mail-Verkehrs mit einem bestimmten Kunden

Eine häufige Art der Nutzung von Verschlüsselungsfunktionen besteht in der Konfiguration einer Richtlinie, die festlegt, dass die Verschlüsselung nur für E-Mail-Nachrichten an einen bestimmten Kunden verwendet werden soll.

Die folgenden Vorgehensweisen zeigen auf, wie das McAfee Email Gateway so konfiguriert wird, dass alle E-Mail-Nachrichten, die an einen bestimmten Kunden gerichtet sind, verschlüsselt gesendet werden.

Vorgehensweise – Erstellen einer neuen Richtlinie

Erfahren Sie, wie Sie eine neue Scan-Richtlinie erstellen können.

Ihre Appliance scannt die über sie versendeten E-Mail-Nachrichten anhand der von Ihnen erstellten Richtlinien. Sie können mehrere Richtlinien erstellen, um zu steuern, wie unterschiedliche Benutzer E-Mail verwenden, oder um verschiedene Aktionen anzugeben, die abhängig von verschiedenen Bedingungen ausgeführt werden sollen.

Vorgehensweise

1. Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien.**
2. Wählen Sie das erforderliche Protokoll aus, indem Sie die Schritte unter *Vorgehensweise – Anzeigen der Richtlinien für SMTP, POP3 bzw. McAfee Secure Web Mail* ausführen.
3. Klicken Sie auf **Richtlinie hinzufügen**.
4. Geben Sie auf der Seite **Scan-Richtlinien – Neue Richtlinie** folgende Informationen an:
   a. Einen Namen für die Richtlinie.
   b. Geben Sie eine optionale Beschreibung für die neue Richtlinie ein.
   c. Geben Sie an, woher sich die Einstellungen der neuen Richtlinie ableiten.

      
      Wenn Sie bereits eine ähnliche Richtlinie eingerichtet haben, wählen Sie diese aus, um deren Einstellungen in die neue Richtlinie zu übernehmen.

   d. Wählen Sie aus, ob die Richtlinie auf ein- oder ausgehenden E-Mail-Verkehr angewendet werden soll. (Nur SMTP)
   e. Wählen Sie die erforderliche **Übereinstimmungs-Logik** für die Richtlinie aus.
   f. Wählen Sie den Regeltyp aus, wählen Sie, wie die Regel übereinstimmen sollte, und wählen Sie den Wert aus, gegen den die Regel testet.
   g. Falls erforderlich, fügen Sie zusätzliche Regeln hinzu, und verwenden Sie die Schaltflächen ⇧ und ⇩, um die Regeln in die richtige Reihenfolge zu bringen.
5. Klicken Sie auf **OK**.

Die neue Richtlinie wird an den Anfang der Richtlinienliste gesetzt.

Vorgehensweise – Konfigurieren der Verschlüsselungseinstellungen

Konfigurieren Sie das McAfee Email Gateway für die Verwendung von Verschlüsselung.

Vorgehensweise

1. Wählen Sie **E-Mail | Verschlüsselung | Secure Web Mail | Grundlegende Einstellungen.**
2. Wählen Sie **Secure Web Mail-Client aktivieren.**
3. Wählen Sie **E-Mail | Verschlüsselung | Secure Web Mail | Benutzerkontoeinstellungen.**

   
   Empfänger werden automatisch angemeldet und erhalten eine digital signierte Benachrichtigung im HTML-Format. Der Administrator wählt, ob eine Push- und/oder eine Pull-Verschlüsselung vorgenommen wird.

4. Wählen Sie **E-Mail | Verschlüsselung | Secure Web Mail | Kennwortverwaltung.**

   
   Die minimale Kennwortlänge beträgt acht Zeichen. Das Kennwort läuft nach 365 Tagen ab.

Task – Aktivieren der Verschlüsselung für Nachrichten, die mit einer Compliance-Regel übereinstimmen

Aktivieren Sie die erforderliche Verschlüsselungsfunktion auf Ihrem McAfee Email Gateway für Nachrichten, die mit einer Compliance-Regel übereinstimmen.

In diesem Beispiel werden Nachrichten verschlüsselt, die mit der HIPAA-Compliance-Regel übereinstimmen.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance**.
2. Klicken Sie auf **Compliance aktivieren**, und wählen Sie **Neue Regel aus Vorlage erstellen**.
3. Suchen Sie die Regel **HIPAA-Compliance**, und wählen Sie sie aus.
4. Klicken Sie auf **Weiter**, um jeweils zur nächsten Assistentenseite zu gelangen.
5. Wählen Sie als primäre Aktion **Durchlassen (Überwachen)**.
6. Wählen Sie unter **Und auch** die Option **Nachricht verschlüsselt zustellen**.
7. Klicken Sie auf **Fertigstellen**, und klicken Sie dann auf **OK**, um das Dialogfeld zu schließen.
8. Wählen Sie **Email | Email Policies | Policy Options | Encryption**.
9. Wählen Sie unter **Verschlüsselungszeitpunkt** die Option **Nur wenn von einer Scan-Aktion ausgelöst**.
10. Wählen Sie unter **Optionen zur integrierten Verschlüsselung** die Option **Secure Web Mail**, und klicken Sie auf **OK**.
11. Übernehmen Sie die Änderungen.

Vorgehensweise – Erkennen von isolierten E-Mail-Nachrichten

Gehen Sie wie nachfolgend beschrieben vor, um nach E-Mails zu suchen, die von Ihrer McAfee Email Gateway Appliance isoliert wurden.

So zeigen Sie eine Liste aller isolierten Nachrichten an:

Vorgehensweise

1. Klicken Sie auf **Berichte | Nachrichtensuche**.
2. Wählen Sie **Isoliert** in der Dropdown-Liste **Nachrichtenstatus** aus.
3. Klicken Sie auf **Suchen/Aktualisieren**.

Alle isolierten Nachrichten werden im unteren Bereich der Seite angezeigt.

Vorgehensweise – Eingrenzen der Suche

Sie können die Suche nach isolierten E-Mails weiter eingrenzen, sodass nur Nachrichten angezeigt werden, die aufgrund von bestimmten Auslösern isoliert wurden. Gehen Sie in diesem Beispiel wie folgt vor, um die E-Mails zu finden, die aufgrund von Compliance-Problemen in die Quarantäne verschoben wurden:

Vorgehensweise

1. Führen Sie die unter *Vorgehensweise – Ermitteln, welche E-Mails isoliert sind* beschriebenen Schritte aus.
2. Wählen Sie **Compliance** in der Dropdown-Liste **Kategorie** aus.
3. Klicken Sie auf **Suchen/Aktualisieren**.

Der untere Bereich des Bildschirms wird aktualisiert und zeigt nur die Nachrichten an, die aufgrund von Compliance-Problemen isoliert wurden.

Vorgehensweise – Anzeigen einer bestimmten E-Mail-Nachricht

Sie können den Inhalt einer isolierten E-Mail sehen.

Vorgehensweise

1. Führen Sie die Schritte unter *Vorgehensweise – Eingrenzen der Suche* aus.
2. Aktivieren Sie links auf der Seite das Kontrollkästchen, um die entsprechende isolierte Nachricht auszuwählen.
3. Klicken Sie auf **Nachricht anzeigen**.

Die ausgewählte Nachricht wird in einem neuen Fenster angezeigt. In diesem Fenster können Sie den Inhalt der E-Mail lesen. Außerdem können Sie alternativ die detaillierten Informationen des E-Mail-Headers anzeigen. Nachdem Sie die Nachricht gelesen haben, können Sie weitere Aktionen für die E-Mail auswählen, indem Sie auf die entsprechenden Schaltflächen klicken.

Vorgehensweise – Freigeben einer isolierten E-Mail-Nachricht

Nachdem Sie die isolierte E-Mail-Nachricht gesehen haben, möchten Sie möglicherweise die Nachricht aus der Quarantäne freigeben. Gehen Sie dazu folgendermaßen vor.

So entlassen Sie eine ausgewählte Nachricht aus der Quarantäne

Vorgehensweise

1. Führen Sie die Schritte unter *Vorgehensweise – Anzeigen einer bestimmten E-Mail-Nachricht* aus.
2. Klicken Sie auf **Ausgewählte Elemente aus Quarantäne entlassen**.

Die ausgewählte E-Mail wird aus der Quarantäne entlassen.



E-Mails mit infiziertem Inhalt können nicht aus der Quarantäne entlassen werden, da dies Schäden auf Ihren Systemen verursachen könnte.

Compliance-Einstellungen

Über diese Seite können Sie Compliance-Regeln erstellen und verwalten.



Email | **Email Policies** | **Compliance** | **Compliance**

Vorteile der Compliance-Einstellungen

Verwenden Sie Compliance-Scans zur Unterstützung der Compliance mit gesetzlichen und betrieblichen Auflagen. Sie können aus einer Bibliothek aus vordefinierten Compliance-Regeln wählen oder eigene Regeln und Wörterbücher für Ihr Unternehmen erstellen.

Compliance-Regeln können hinsichtlich ihrer Komplexität von einem einfachen Auslöser bei der Erkennung eines einzelnen Begriffs in einem Wörterbuch bis hin zum Aufbauen auf und Kombinieren von faktorbasierten Wörterbüchern variieren, die nur auslösen, wenn ein bestimmter Schwellenwert erreicht wird. Mithilfe der erweiterten Funktionen von Compliance-Regeln können Wörterbücher mit den logischen Operationen *eines von*, *alle von* oder *außer* kombiniert werden.

Vorgehensweise – Beschränken des Faktorbeitrags eines Wörterbuchbegriffs

Gehen Sie wie nachfolgend beschrieben vor, um den Faktorbeitrag eines Wörterbuchbegriffs zu beschränken.

> **Bevor Sie beginnen**
>
> Bei dieser Vorgehensweise wird davon ausgegangen, dass Ihre Regel ein Wörterbuch enthält, das die Aktion basierend auf einem Schwellenwert auslöst, beispielsweise das Wörterbuch **Vergütung und Leistungen**.

Sie können beschränken, wie oft ein Begriff zum Gesamtfaktor beitragen kann.

Wenn beispielsweise "Testbegriff" in einem Wörterbuch den Faktor 10 hat und fünfmal in einer E-Mail erkannt wird, wird 50 zum Gesamtfaktor addiert. Alternativ können Sie eine Beschränkung festlegen, sodass beispielsweise nur zwei Vorkommnisse zum Gesamtwert beitragen, indem Sie für "Max. Begriffsanzahl" den Wert "2" angeben.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance**.
2. Erweitern Sie die Regel, die Sie bearbeiten möchten, und klicken Sie anschließend auf das Symbol **Bearbeiten** neben dem Wörterbuch, dessen Faktor Sie ändern möchten.
3. Geben Sie unter **Max. Begriffsanzahl** die maximale Anzahl an Vorkommnissen eines Begriffs an, die zum Gesamtfaktor beitragen sollen.

Vorgehensweise – Bearbeiten des einer vorhandenen Regel zugewiesenen Schwellenwerts

Gehen Sie wie nachfolgend beschrieben vor, um den Schwellenwert zu bearbeiten, der einer vorhandenen Regel zugeordnet ist.

> **Bevor Sie beginnen**
>
> Bei dieser Vorgehensweise wird davon ausgegangen, dass Ihre Regel ein Wörterbuch enthält, das die Aktion basierend auf einem Schwellenwert auslöst, beispielsweise das Wörterbuch **Vergütung und Leistungen**.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance**.
2. Erweitern Sie die Regel, die Sie bearbeiten möchten, und wählen Sie anschließend das Symbol **Bearbeiten** neben dem Wörterbuch aus, dessen Faktor Sie ändern möchten.
3. Geben Sie unter **Schwellenwert für Wörterbuch** den Faktor ein, bei dem die Regel ausgelöst werden soll, und klicken Sie auf **OK**.

Vorgehensweise – Definieren einer Regel zum Überwachen oder Blockieren bei Erreichen eines Schwellenwerts

Bei faktorbasierten Wörterbüchern kann es sinnvoll sein, Auslöser zu überwachen, die einen niedrigen Schwellenwert erreichen, und die E-Mails nur zu blockieren, wenn ein hoher Schwellenwert erreicht wird.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance**.
2. Klicken Sie auf **Neue Regel erstellen**, geben Sie einen Namen für die Regel ein, beispielsweise `Unzufriedenheit - Niedrig`, und klicken Sie auf **Weiter**.
3. Wählen Sie das Wörterbuch **Unzufriedenheit** aus, und geben Sie unter **Schwellenwert** den Wert `20` ein.
4. Klicken Sie auf **Weiter** und anschließend erneut auf **Weiter**.
5. Akzeptieren Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Standardaktion.
6. Klicken Sie auf **Fertig stellen**.
7. Wiederholen Sie die Schritte 2 bis 4, um eine weitere neue Regel zu erstellen. Nennen Sie diese jedoch `Unzufriedenheit - Hoch`, und weisen Sie ihr den Schwellenwert 40 zu.
8. Wählen Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Option **Verbindung verweigern (Blockieren)** aus.
9. Klicken Sie auf **Fertig stellen**.
10. Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

Vorgehensweise – Hinzufügen eines Wörterbuchs zu einer Regel

Gehen Sie wie folgt vor, um ein neues Wörterbuch zu einer vorhandenen Regel hinzuzufügen.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance**.
2. Erweitern Sie die Regel, die Sie bearbeiten möchten.
3. Wählen Sie **Wörterbuch hinzufügen**.
4. Wählen Sie das neue Wörterbuch aus, das Sie hinzufügen möchten, und klicken Sie auf **OK**.

Vorgehensweise – Erstellen einer komplexen benutzerdefinierten Regel

Gehen Sie wie nachfolgend beschrieben vor, um eine komplexe Regel zu erstellen, die auslöst, wenn sowohl Wörterbuch A als auch Wörterbuch B erkannt werden, jedoch nicht, wenn darüber hinaus auch Wörterbuch C erkannt wird.

Vorgehensweise

1. Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien** , und wählen Sie **Compliance**.
2. Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Neue Regel erstellen**, um den **Assistenten für die Regelerstellung** zu öffnen.
4. Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.
5. Wählen Sie zwei Wörterbücher aus, die in die Regel aufgenommen werden sollen, und klicken Sie auf **Weiter**.
6. Wählen Sie in der Ausschlussliste ein Wörterbuch aus, das Sie von der Regel ausschließen möchten.
7. Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn die Regel ausgelöst wird.
8. Wählen Sie in der Dropdown-Liste **Und bedingt** die Option **Alle** aus, und klicken Sie auf **Fertig stellen**.

Vorgehensweise – Erstellen einer einfachen benutzerdefinierten Regel

Gehen Sie wie nachfolgend beschrieben vor, um eine einfache benutzerdefinierte Regel zu erstellen, die Nachrichten blockiert, die Sozialversicherungsnummern enthalten.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance**.
2. Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Neue Regel erstellen**, um den **Assistenten für die Regelerstellung** zu öffnen.
4. Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.
5. Geben Sie im Suchfeld `sozial` ein.
6. Wählen Sie das Wörterbuch **Sozialversicherungsnummer** aus, und klicken Sie zweimal auf **Weiter**.
7. Wählen Sie die Aktion **Verbindung verweigern (Blockieren)** aus, und klicken Sie auf **Fertig stellen**.

Vorgehensweise – Blockieren von Nachrichten, die gegen eine Richtlinie verstoßen

Gehen Sie wie nachfolgend beschrieben vor, um E-Mail-Nachrichten zu blockieren, die die Richtlinie "Bedrohliche Sprache" verletzen.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance**.
2. Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Neue Regel aus Vorlage erstellen**, um den **Assistent für die Regelerstellung** zu öffnen.
4. Wählen Sie die Richtlinie **Zulässige Nutzung - Bedrohliche Sprache** aus, und klicken Sie auf **Weiter**.
5. Sie können den Namen der Regel optional ändern. Klicken Sie anschließend auf **Weiter**.
6. Ändern Sie die primäre Aktion in **Verbindung verweigern (Blockieren)**, und klicken Sie auf **Fertig stellen**.
7. Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

Data Loss Prevention-Einstellungen

Auf dieser Seite können Sie eine Richtlinie erstellen, die Data Loss Prevention-Aktionen für die Kategorien der registrierten Dokumente zuweist.


Email | Email Policies | Compliance | Data Loss Prevention

Vorteile des Einsatzes von Data Loss Prevention (DLP)

Mit der Data Loss Prevention-Funktion können Sie den Fluss kritischer Informationen beschränken, die in E-Mail-Nachrichten per SMTP über die Appliance gesendet werden. Sie können beispielsweise die Übertragung eines kritischen Dokuments, wie z. B. eines Finanzberichts, blockieren, das an eine Adresse außerhalb Ihres Unternehmens gesendet werden soll. Die Erkennung erfolgt, sobald das Originaldokument als E-Mail-Anhang oder als Textausschnitt aus dem Originaldokument versendet wird.

Die DLP-Konfiguration erfolgt in zwei Phasen:

- Registrierung der Dokumente, die geschützt werden sollen
- Aktivieren der DLP-Richtlinie und Kontrollieren der Erkennung (dieses Thema)



Wenn ein hochgeladenes registriertes Dokument eingebettete Dokumente enthält, wird von deren Inhalt ebenfalls ein Fingerabdruck angelegt. Wenn später während eines Scans der Übereinstimmungsprozentsatz berechnet wird, wird der kombinierte Inhalt verwendet. Wenn eingebettete Dokumente separat behandelt werden sollen, müssen sie separat registriert werden.

Vorgehensweise – Verhindern, dass ein vertrauliches Dokument gesendet wird

Im Folgenden erfahren Sie, wie Sie verhindern, dass vertrauliche Finanzdokumente aus Ihrem Unternehmen heraus gesendet werden.

Bevor Sie beginnen

In diesem Beispiel wird davon ausgegangen, dass Sie bereits die Kategorie "Finanzen" erstellt haben.

Vorgehensweise

1. Wählen Sie **Email** | **Email Policies** | **Compliance** | **Data Loss Prevention**.
2. Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Neue Regel erstellen**, wählen Sie die Kategorie "Finanzen" aus, und klicken Sie auf **OK**, damit die Kategorie in der Liste **Regeln** angezeigt wird.
4. Wählen Sie die der Kategorie zugeordnete Aktion aus, ändern Sie die primäre Aktion in **Verbindung verweigern (Blockieren)**, und klicken Sie auf **OK**.
5. Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

Vorgehensweise – Blockieren des Versendens eines Dokumentabschnitts

Gehen Sie wie nachfolgend beschrieben vor, um zu verhindern, dass auch nur ein kleiner Abschnitt eines Dokuments aus Ihrem Unternehmen heraus gesendet wird.

Vorgehensweise

1. Wählen Sie **Email** | **Email Policies** | **Compliance** | **Data Loss Prevention**.
2. Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.
3. Aktivieren Sie die Einstellung für aufeinander folgende Signaturen, und geben Sie die Anzahl an aufeinander folgende Signaturen ein, bei der die DLP-Richtlinie eine Erkennung auslösen soll. Der Standardwert ist **10**.
4. Klicken Sie auf **Neue Regel erstellen**, wählen Sie die Kategorie "Finanzen" aus, und klicken Sie auf **OK**, damit die Kategorie in der Liste "Regeln" angezeigt wird.
5. Wählen Sie die der Kategorie zugeordnete Aktion aus, ändern Sie die primäre Aktion in **Verbindung verweigern (Blockieren)**, und klicken Sie auf **OK**.
6. Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

Vorgehensweise – Ausschließen eines bestimmten Dokuments für eine Richtlinie

Gehen Sie wie nachfolgend beschrieben vor, um zu verhindern, dass ein bestimmtes Finanzdokument die DLP-Richtlinieneinstellungen auslöst.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance | Data Loss Prevention**.
2. Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Dokumentausschluss erstellen**, wählen Sie das Dokument aus, das von dieser Richtlinie ignoriert werden soll, und klicken Sie auf **OK**.
4. Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

Index

700-3339B15

